Legal Notice

Copyright © 2000-2016 EMC Corporation. All Rights Reserved.

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. Adobe and Adobe PDF Library are trademarks or registered trademarks of Adobe Systems Inc. in the U.S. and other countries. All other trademarks used herein are the property of their respective owners.

Documentation Feedback

Your opinion matters. We want to hear from you regarding our product documentation. If you have feedback about how we can make our documentation better or easier to use, please send us your feedback directly at IIGDocumentationFeedback@emc.com
# Table of Contents

<table>
<thead>
<tr>
<th>Chapter</th>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Preface</td>
<td>Documentum Administrator</td>
<td>23</td>
</tr>
<tr>
<td>Chapter 1</td>
<td>Documentum Administrator</td>
<td>25</td>
</tr>
<tr>
<td></td>
<td>Documentum Administrator</td>
<td>25</td>
</tr>
<tr>
<td></td>
<td>Logging in to Documentum Administrator</td>
<td>25</td>
</tr>
<tr>
<td></td>
<td>The System Information page</td>
<td>27</td>
</tr>
<tr>
<td></td>
<td>Determining the Documentum Administrator version</td>
<td>29</td>
</tr>
<tr>
<td></td>
<td>Preferences</td>
<td>29</td>
</tr>
<tr>
<td>Chapter 2</td>
<td>Basic Configuration</td>
<td>31</td>
</tr>
<tr>
<td></td>
<td>Adding a connection broker for one session</td>
<td>31</td>
</tr>
<tr>
<td></td>
<td>Configuring licenses</td>
<td>32</td>
</tr>
<tr>
<td></td>
<td>Enabling a feature or product</td>
<td>32</td>
</tr>
<tr>
<td></td>
<td>Tracking software usage and AMP</td>
<td>33</td>
</tr>
<tr>
<td></td>
<td>Managing repositories</td>
<td>33</td>
</tr>
<tr>
<td></td>
<td>Viewing or modifying the repository configuration</td>
<td>34</td>
</tr>
<tr>
<td></td>
<td>Modifying repository synchronization</td>
<td>40</td>
</tr>
<tr>
<td></td>
<td>Moving a repository to dormant and active states</td>
<td>41</td>
</tr>
<tr>
<td></td>
<td>Enabling a repository as a global registry</td>
<td>42</td>
</tr>
<tr>
<td></td>
<td>Repository content</td>
<td>43</td>
</tr>
<tr>
<td></td>
<td>Type indexes</td>
<td>44</td>
</tr>
<tr>
<td></td>
<td>Date values</td>
<td>45</td>
</tr>
<tr>
<td></td>
<td>Moving or duplicating a repository</td>
<td>45</td>
</tr>
<tr>
<td></td>
<td>Supporting object types</td>
<td>46</td>
</tr>
<tr>
<td></td>
<td>Dumping objects under retention</td>
<td>46</td>
</tr>
<tr>
<td></td>
<td>Aspects and dump operations</td>
<td>46</td>
</tr>
<tr>
<td></td>
<td>Dumping an entire repository</td>
<td>47</td>
</tr>
<tr>
<td></td>
<td>Dumping specific objects</td>
<td>47</td>
</tr>
<tr>
<td></td>
<td>Setting the type property</td>
<td>47</td>
</tr>
<tr>
<td></td>
<td>Setting the predicate properties</td>
<td>48</td>
</tr>
<tr>
<td></td>
<td>Content files and dumping</td>
<td>49</td>
</tr>
<tr>
<td></td>
<td>Dumping without content</td>
<td>49</td>
</tr>
<tr>
<td></td>
<td>Including content</td>
<td>49</td>
</tr>
<tr>
<td></td>
<td>Compressing content</td>
<td>49</td>
</tr>
<tr>
<td></td>
<td>Setting the cache size</td>
<td>50</td>
</tr>
<tr>
<td></td>
<td>Using non-restartable dump</td>
<td>50</td>
</tr>
<tr>
<td></td>
<td>Using a script to create a dump file</td>
<td>50</td>
</tr>
<tr>
<td></td>
<td>Sample script for a partial repository dump</td>
<td>51</td>
</tr>
<tr>
<td></td>
<td>If the server crashes during a dump operation</td>
<td>53</td>
</tr>
<tr>
<td></td>
<td>Moving the dump file</td>
<td>53</td>
</tr>
<tr>
<td></td>
<td>Loading a repository</td>
<td>53</td>
</tr>
<tr>
<td></td>
<td>Refreshing repository objects from a dump file</td>
<td>54</td>
</tr>
<tr>
<td></td>
<td>Loading job objects</td>
<td>54</td>
</tr>
<tr>
<td></td>
<td>Loading registered tables</td>
<td>54</td>
</tr>
<tr>
<td></td>
<td>Turning off save event generation during load operations</td>
<td>54</td>
</tr>
<tr>
<td></td>
<td>Loading a new repository</td>
<td>55</td>
</tr>
<tr>
<td></td>
<td>The preLoad utility</td>
<td>55</td>
</tr>
<tr>
<td>Contents</td>
<td>Page</td>
<td></td>
</tr>
<tr>
<td>-------------------------------------------------------------------------</td>
<td>------</td>
<td></td>
</tr>
<tr>
<td>Load procedure for new repositories</td>
<td>55</td>
<td></td>
</tr>
<tr>
<td>DocApps</td>
<td>57</td>
<td></td>
</tr>
<tr>
<td>Generating dump and load trace messages</td>
<td>57</td>
<td></td>
</tr>
<tr>
<td>Repository maintenance</td>
<td>57</td>
<td></td>
</tr>
<tr>
<td>Checking consistency</td>
<td>59</td>
<td></td>
</tr>
<tr>
<td>Running the job from a command line</td>
<td>59</td>
<td></td>
</tr>
<tr>
<td>Changing the repository owner password</td>
<td>64</td>
<td></td>
</tr>
<tr>
<td>Windows domain authentication for Linux repositories</td>
<td>65</td>
<td></td>
</tr>
<tr>
<td>Creating or modifying a domain map</td>
<td>65</td>
<td></td>
</tr>
<tr>
<td>Defining a domain</td>
<td>66</td>
<td></td>
</tr>
<tr>
<td>Modifying users for Windows domain authentication</td>
<td>66</td>
<td></td>
</tr>
<tr>
<td>Managing Content Servers</td>
<td>67</td>
<td></td>
</tr>
<tr>
<td>Adding or modifying Content Servers</td>
<td>68</td>
<td></td>
</tr>
<tr>
<td>Duplicating a server configuration object</td>
<td>69</td>
<td></td>
</tr>
<tr>
<td>Modifying general server configuration information</td>
<td>70</td>
<td></td>
</tr>
<tr>
<td>Creating or modifying connection broker projections</td>
<td>75</td>
<td></td>
</tr>
<tr>
<td>Creating or modifying network locations</td>
<td>76</td>
<td></td>
</tr>
<tr>
<td>Creating or modifying application servers</td>
<td>77</td>
<td></td>
</tr>
<tr>
<td>Creating or modifying cached types</td>
<td>78</td>
<td></td>
</tr>
<tr>
<td>Creating or modifying locations</td>
<td>78</td>
<td></td>
</tr>
<tr>
<td>Creating or modifying far stores</td>
<td>79</td>
<td></td>
</tr>
<tr>
<td>Moving a server to dormant and active states</td>
<td>80</td>
<td></td>
</tr>
<tr>
<td>Enabling or disabling save operation for a Content Server in dormant state</td>
<td>81</td>
<td></td>
</tr>
<tr>
<td>Projecting active or dormant state of Content Server to connection broker</td>
<td>82</td>
<td></td>
</tr>
<tr>
<td>Viewing server and connection broker log files</td>
<td>83</td>
<td></td>
</tr>
<tr>
<td>Deleting a server configuration object</td>
<td>84</td>
<td></td>
</tr>
<tr>
<td>Confirming object deletion</td>
<td>84</td>
<td></td>
</tr>
<tr>
<td>Configuring a server as a process engine</td>
<td>85</td>
<td></td>
</tr>
<tr>
<td>Disabling a process engine server</td>
<td>85</td>
<td></td>
</tr>
<tr>
<td>Federations</td>
<td>85</td>
<td></td>
</tr>
<tr>
<td>Creating or modifying federations</td>
<td>86</td>
<td></td>
</tr>
<tr>
<td>Adding, modifying, or deleting federation members</td>
<td>88</td>
<td></td>
</tr>
<tr>
<td>Deleting Federations</td>
<td>88</td>
<td></td>
</tr>
<tr>
<td>Connecting to the governing repository or a federation member</td>
<td>89</td>
<td></td>
</tr>
<tr>
<td>Choosing user subtypes</td>
<td>89</td>
<td></td>
</tr>
<tr>
<td>Choosing repository federation members</td>
<td>89</td>
<td></td>
</tr>
<tr>
<td>Java Method Servers</td>
<td>90</td>
<td></td>
</tr>
<tr>
<td>Viewing Java method server information</td>
<td>90</td>
<td></td>
</tr>
<tr>
<td>Modifying a Java Method Server configuration</td>
<td>91</td>
<td></td>
</tr>
<tr>
<td>Adding or modifying associated Content Servers</td>
<td>92</td>
<td></td>
</tr>
<tr>
<td>Viewing active Java method servers</td>
<td>93</td>
<td></td>
</tr>
<tr>
<td>LDAP servers</td>
<td>94</td>
<td></td>
</tr>
<tr>
<td>Viewing LDAP server configurations</td>
<td>95</td>
<td></td>
</tr>
<tr>
<td>Adding or modifying LDAP server configurations</td>
<td>96</td>
<td></td>
</tr>
<tr>
<td>LDAP Server Configuration properties</td>
<td>97</td>
<td></td>
</tr>
<tr>
<td>LDAP Server Sync &amp; Authentication properties</td>
<td>100</td>
<td></td>
</tr>
<tr>
<td>LDAP Server mapping properties</td>
<td>101</td>
<td></td>
</tr>
<tr>
<td>LDAP Server failover properties</td>
<td>103</td>
<td></td>
</tr>
<tr>
<td>Mapping LDAP Servers</td>
<td>104</td>
<td></td>
</tr>
<tr>
<td>Mapping guidelines</td>
<td>105</td>
<td></td>
</tr>
<tr>
<td>Using Search Builder</td>
<td>105</td>
<td></td>
</tr>
<tr>
<td>Adding or modifying repository property mapping</td>
<td>105</td>
<td></td>
</tr>
<tr>
<td>Configuring secondary LDAP servers</td>
<td>106</td>
<td></td>
</tr>
<tr>
<td>Changing the binding password</td>
<td>107</td>
<td></td>
</tr>
<tr>
<td>Forcing LDAP server synchronization</td>
<td>107</td>
<td></td>
</tr>
</tbody>
</table>
Chapter 3  Distributed Configurations  ................................................................. 113  
Network locations ...................................................................................... 113  
Creating, viewing, or modifying network locations .................................. 114  
Copying network locations ....................................................................... 115  
Deleting network locations ....................................................................... 116  
ACS servers .................................................................................................. 117  
Viewing or modifying the ACS server configuration properties .......... 118  
ACS projections and stores ........................................................................ 120  
Designating connection brokers for an ACS server .................................. 122  
Choosing network locations ...................................................................... 123  
BOCS servers ............................................................................................... 123  
Creating, viewing, or modifying BOCS servers ....................................... 124  
Setting BOCS server security .................................................................... 126  
Setting BOCS server communication protocols ....................................... 127  
Deleting BOCS servers ............................................................................... 128  
Configuring distributed transfer settings .................................................. 128  
Messaging server configuration ................................................................. 130  

Chapter 4  User Management .................................................................... 133  
Administering users, groups, roles, and sessions ....................................... 133  
Users ............................................................................................................ 134  
Locating users ............................................................................................ 134  
Creating or modifying users ....................................................................... 135  
Creating global users .................................................................................. 140  
Setting default permissions for folders and cabinets ................................ 140  
Importing users ............................................................................................ 141  
Import file format ....................................................................................... 144  
Deleting users .............................................................................................. 145  
Reassigning objects to another user ........................................................ 145  
Changing the home repository of a user .................................................. 146  
Activating or deactivating a user account ................................................ 146  
Viewing groups, workflows, alias sets, permission sets, and documents of a user ............................................................... 147  
Viewing or deleting change home repository logs .................................... 147  
Viewing user reassign logs ......................................................................... 147  
Reassign reports .......................................................................................... 148  
Groups .......................................................................................................... 148  
Dynamic groups ......................................................................................... 149  
Privileged groups ........................................................................................ 149  
Locating groups .......................................................................................... 151  
Viewing group memberships ..................................................................... 151  
Creating, viewing, or modifying groups .................................................. 151  
Adding users, groups, or roles to a group .................................................. 153  
Removing users from a group ..................................................................... 154
Auditing
Deleting
Adding
Killing
Adding, Deleting
Audit
Permission Management
roles by
user groups audits modifying, object permission type sessions validation instance roles information set (dm _)
AuditMgt)

Chapter 5  Security .................................................................................................................. 165
Permission sets ....................................................................................................................... 165
Locating a permission set ........................................................................................................ 165
Creating, viewing, or modifying permission sets ................................................................ 166
Adding, viewing, or modifying permissions for a permission set ........................................ 167
Copying a permission set ........................................................................................................ 169
Adding users to permission sets ............................................................................................ 170
Deleting users from permission sets ...................................................................................... 171
Deleting a permission set ........................................................................................................ 171
Assigning basic and extended object permissions ............................................................... 171
Permission set associations ..................................................................................................... 173
Changing the permissions assigned to a user ........................................................................ 173
Permission set validation ......................................................................................................... 174

Chapter 6  Audit Management ................................................................................................. 175
Auditing ................................................................................................................................... 175
Auditing by object type ........................................................................................................... 176
Choosing a type ....................................................................................................................... 177
Auditing by object instance ..................................................................................................... 178
Auditing by events selected for all objects in the repository .................................................. 179
Search audit ............................................................................................................................. 180
Audit policies ........................................................................................................................... 181
Creating, modifying, or deleting an audit policy ................................................................... 182
Audit Policy example ............................................................................................................... 182
Registering audits .................................................................................................................... 183
Adding, modifying, or removing audits .................................................................................. 184
Verifying or purging audit trails .............................................................................................. 184

Chapter 7  Job Management .................................................................................................... 187
Jobs .......................................................................................................................................... 187
Job descriptions ...................................................................................................................... 188
ACL replication (dm_ACLReplication) .................................................................................... 189
ACL replication (dm_ACLRepl_repository) ............................................................................. 189
Asynchronous Write (dm_AsynchronousWrite) ...................................................................... 189
Audit management (dm_AuditMgt) ......................................................................................... 189
<table>
<thead>
<tr>
<th>Topic</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Consistency checker (dm_ConsistencyChecker)</td>
<td>190</td>
</tr>
<tr>
<td>Content replication (dm_ContentReplication)</td>
<td>191</td>
</tr>
<tr>
<td>Content warning (dm_ContentWarning)</td>
<td>191</td>
</tr>
<tr>
<td>Data dictionary publisher (dm_DataDictionaryPublisher)</td>
<td>191</td>
</tr>
<tr>
<td>Database space warning (dm_DBWarning)</td>
<td>192</td>
</tr>
<tr>
<td>Distributed operations (dm_DistOperations)</td>
<td>192</td>
</tr>
<tr>
<td>Archive (dm_DMArchive)</td>
<td>192</td>
</tr>
<tr>
<td>Dmclean (dm_DMClean)</td>
<td>192</td>
</tr>
<tr>
<td>Dmfilescan (dm_Dmfilescan)</td>
<td>193</td>
</tr>
<tr>
<td>Federation copy (dm_FederationCopy)</td>
<td>193</td>
</tr>
<tr>
<td>Federation export (dm_FederationExport)</td>
<td>193</td>
</tr>
<tr>
<td>Federation import (dm_FederationImport)</td>
<td>193</td>
</tr>
<tr>
<td>Federation status (dm_FederationStatus)</td>
<td>194</td>
</tr>
<tr>
<td>Federation update (dm_FederationUpdate)</td>
<td>194</td>
</tr>
<tr>
<td>File report (dm_FileReport)</td>
<td>194</td>
</tr>
<tr>
<td>Group rename (dm_GroupRename and dm_GroupRename_Java)</td>
<td>194</td>
</tr>
<tr>
<td>LDAP synchronization (dm_LDAPSynchronization)</td>
<td>195</td>
</tr>
<tr>
<td>Log purge (dm_LogPurge)</td>
<td>196</td>
</tr>
<tr>
<td>Queue management (dm_QueueMgt)</td>
<td>196</td>
</tr>
<tr>
<td>Remove expired retention objects (dm_RemoveExpiredRetnObjects)</td>
<td>197</td>
</tr>
<tr>
<td>Rendition manager (dm_RenditionMgt)</td>
<td>198</td>
</tr>
<tr>
<td>SCS log purge (dm_SCSLogPurgeJob)</td>
<td>198</td>
</tr>
<tr>
<td>State of repository report (dm_StateOfDocbase)</td>
<td>198</td>
</tr>
<tr>
<td>Swap info (dm_SwapInfo)</td>
<td>199</td>
</tr>
<tr>
<td>Update statistics (dm_UpdateStats)</td>
<td>199</td>
</tr>
<tr>
<td>Usage tracking (dm_usageReport)</td>
<td>199</td>
</tr>
<tr>
<td>User change home repository (dm_UserChgHomeDb and</td>
<td>200</td>
</tr>
<tr>
<td>dm_UserChgHomeDB_Java)</td>
<td></td>
</tr>
<tr>
<td>User rename (dm_UserRename and dm_UserRename_Java)</td>
<td>200</td>
</tr>
<tr>
<td>Version management (dm_VersionMgt)</td>
<td>201</td>
</tr>
<tr>
<td>WfmsTimer (dm_WfmsTimer)</td>
<td>201</td>
</tr>
<tr>
<td>Creating a job</td>
<td>201</td>
</tr>
<tr>
<td>Changing the schedule of a job</td>
<td>203</td>
</tr>
<tr>
<td>Setting the qualifier rules for the remove retention-expired objects</td>
<td>204</td>
</tr>
<tr>
<td>Job</td>
<td>205</td>
</tr>
<tr>
<td>Assigning a method to a job</td>
<td>205</td>
</tr>
<tr>
<td>Locating a method for a job</td>
<td>207</td>
</tr>
<tr>
<td>Creating, viewing, or modifying SysObject properties</td>
<td>207</td>
</tr>
<tr>
<td>Creating replication jobs</td>
<td>208</td>
</tr>
<tr>
<td>Selecting the source repository for a replication job</td>
<td>209</td>
</tr>
<tr>
<td>Selecting the target repository for a replication job</td>
<td>209</td>
</tr>
<tr>
<td>Setting replication job options</td>
<td>210</td>
</tr>
<tr>
<td>Choosing a replication folder</td>
<td>210</td>
</tr>
<tr>
<td>Choosing a replication job user</td>
<td>210</td>
</tr>
<tr>
<td>Choosing a permission set for replica objects</td>
<td>212</td>
</tr>
<tr>
<td>Choosing a storage area</td>
<td>212</td>
</tr>
<tr>
<td>Choosing replication and security modes</td>
<td>213</td>
</tr>
<tr>
<td>Creating records migration jobs</td>
<td>213</td>
</tr>
<tr>
<td>Setting the rules of a records migration job</td>
<td>214</td>
</tr>
<tr>
<td>Defining selection criteria for a records migration job</td>
<td>217</td>
</tr>
<tr>
<td>Defining version criteria for records migration job</td>
<td>218</td>
</tr>
<tr>
<td>Creating remove expired retention objects jobs</td>
<td>219</td>
</tr>
<tr>
<td>Creating BOCS caching jobs</td>
<td>220</td>
</tr>
<tr>
<td>Setting BOCS caching rules</td>
<td>220</td>
</tr>
<tr>
<td>Creating job sequences</td>
<td>222</td>
</tr>
<tr>
<td>Providing repository and job information for a job sequence</td>
<td>223</td>
</tr>
<tr>
<td>Selecting jobs for a job sequence</td>
<td>224</td>
</tr>
<tr>
<td>Setting dependencies for a job sequence</td>
<td>225</td>
</tr>
<tr>
<td>Running jobs</td>
<td>225</td>
</tr>
</tbody>
</table>
Viewing the status of a running job ........................................ 226
Viewing job reports ......................................................... 226
Setting the trace level for a job ............................................ 226
Viewing job trace logs ...................................................... 227
Deleting jobs ...................................................................... 227
Deactivating jobs that fail .................................................. 227
Methods ........................................................................... 228
Creating or modifying methods ............................................. 228
Importing method content .................................................. 231
Running methods ............................................................. 232
Viewing the results of a method .......................................... 233
Exporting method content .................................................. 233
Editing method content ...................................................... 234
Checking in method content ................................................. 234
Deleting methods .............................................................. 235
Administration methods ................................................... 235
Viewing administration methods ......................................... 236
Running administration methods ......................................... 236
CAN_FETCH ...................................................................... 237
CLEAN_LINKS .................................................................. 238
DELETE_REPLICA ........................................................... 238
DESTROY_CONTENT .......................................................... 239
EXPORT_TICKET_KEY ......................................................... 240
GET_PATH ....................................................................... 240
IMPORT_REPLICA .............................................................. 241
IMPORT_TICKET_KEY ........................................................... 241
MIGRATE_CONTENT ............................................................ 242
PURGE_CONTENT ............................................................... 247
REPLICATE ...................................................................... 248
RESTORE_CONTENT ........................................................... 249
SET_STORAGE_STATE ......................................................... 250
DB_STATS ...................................................................... 251
DROP_INDEX ..................................................................... 251
EXEC_SQL ....................................................................... 252
FINISH_INDEX_MOVES ....................................................... 252
GENERATE_PARTITION_SCHEMA_SQL ................................ 253
MAKE_INDEX .................................................................... 255
MOVE_INDEX .................................................................... 256
ESTIMATE_SEARCH ............................................................ 256
MARK_FOR_RETRY .............................................................. 257
MODIFY_TRACE ................................................................ 258
GET_LAST_SQL ................................................................ 258
LIST_RESOURCES ............................................................. 259
LIST_TARGETS ................................................................. 260
SET_OPTIONS .................................................................. 261
RECOVER_AUTO_TASKS ....................................................... 262
WORKFLOW_AGENT_MANAGEMENT .................................... 263
Administration Methods Results Page ............................... 264
Choosing a file on the server file system .............................. 265

**Chapter 8**

**Alias Sets** ..................................................................... 267
Alias sets and aliases ......................................................... 267
Creating or modifying alias sets .......................................... 267
Viewing or removing aliases ................................................. 268
Adding or modifying aliases ............................................... 269
Deleting alias sets ............................................................. 270
Table of Contents

Associating an assignment policy with an object type ........................................... 321
Deleting assignment policies ....................................................................................... 322
Migration policies ........................................................................................................ 322
Creating, viewing, or modifying migration policies .................................................... 323
Configuring a migration policy schedule ..................................................................... 324
Configuring migration policy rules .............................................................................. 324
Configuring migration policy SysObject information .................................................. 326
Viewing migration policy job reports .......................................................................... 327
Deleting migration policies .......................................................................................... 327

Chapter 12  Content Delivery .......................................................................................... 329
Content delivery services ............................................................................................. 329
Locating content delivery configurations ...................................................................... 330
Creating or modifying content delivery configurations ................................................ 331
Configuring the advanced properties of a content delivery configuration .................... 333
Configuring replication properties for a content delivery configuration ....................... 338
Configuring extra arguments for a content delivery configuration ................................ 339
Deleting content delivery configurations ...................................................................... 353
Testing content delivery configurations ....................................................................... 353
Duplicating a content delivery configuration .................................................................. 354
Deactivating a content delivery configuration .............................................................. 354
Publishing objects ........................................................................................................ 355
Content delivery configuration results ........................................................................... 356
Content delivery logs .................................................................................................... 357
Viewing content delivery logs ...................................................................................... 357
Deleting content delivery logs ...................................................................................... 357
Effective labels ............................................................................................................. 358

Chapter 13  Indexing Management .................................................................................. 359
Indexing ....................................................................................................................... 359
Index agents and xPlore ................................................................................................. 359
Starting and stopping index agents .............................................................................. 360
Disabling index agents ................................................................................................. 360
Enabling index agents ................................................................................................. 361
Verifying indexing actions ............................................................................................ 361
Viewing or modifying index agent properties .............................................................. 361
Managing index queue items ....................................................................................... 362
  Resubmitting individual objects ................................................................................. 363
  Resubmitting all failed queue items ............................................................................ 363
Removing queue items by status .................................................................................. 363
Removing queue items ................................................................................................. 364
Viewing queue items associated with an object ............................................................ 364
Creating a new indexing queue item ............................................................................ 364

Chapter 14  Content Transformation Services Management ........................................ 367
Content Transformation Services ................................................................................. 367
Changing the CTS user ................................................................................................. 367
Configuring a CTS instance .......................................................................................... 368
Changing the polling interval ....................................................................................... 368
Chapter 15  Content Intelligence Services ................................................................. 377

Content Intelligence Services in Documentum applications .............................. 377
  Classic categorization in Webtop ................................................................. 378
  Content Intelligence Services in xCP deployments ....................................... 378

Configuring Content Intelligence Services in Documentum Administrator .......................... 379
  Setting up Content Intelligence Services for classic categorization ...................... 379
  Enabling Content Intelligence Services .......................................................... 380
  Defining Content Intelligence Services configuration ....................................... 381
  Data synchronization between the repository and CIS server ............................. 382
  Missing Content Intelligence node .................................................................... 382

Building taxonomies for classic categorization ..................................................... 383
  Taxonomies ........................................................................................................ 384
  Category classes .............................................................................................. 385
  Categories ......................................................................................................... 385
  Taxonomy manager ............................................................................................ 386
  Category owner ................................................................................................ 386
  Viewing taxonomies and categories ................................................................. 386
  Providing evidence ............................................................................................ 387
  Confidence values and score thresholds ........................................................... 388
  Category and taxonomy rules .......................................................................... 389
  Evidence terms ................................................................................................ 390
  Using stemming on evidence terms ................................................................. 390
  Language detection for stemming ................................................................. 391
  Reusing category evidence .............................................................................. 392
  Defining category classes .................................................................................. 392
  Defining taxonomies ......................................................................................... 394
  Defining categories ......................................................................................... 395
  Defining property rules ..................................................................................... 397
  Defining evidence terms ................................................................................... 399
  Synchronizing taxonomies with CIS server ....................................................... 400
  Making taxonomies available ........................................................................... 401
  Setting permissions for Content Intelligence .................................................... 401
  Displaying object titles ..................................................................................... 402
  Displaying attributes in Property rules ............................................................. 402
  Creating subtypes for a taxonomy or a category ............................................... 403
  Deleting category classes .................................................................................. 404
  Deleting taxonomies .......................................................................................... 404
  Selecting and submitting the documents to analyze ........................................... 405
  Document sets ................................................................................................... 405
  Document set language ..................................................................................... 406

EMC Documentum Administrator Version 7.2 User Guide 11
Defining document sets........................................................................... 406
Configuring a document set ........................................................................ 407
Viewing the documents in a document set .................................................. 408
Scheduling a document set .......................................................................... 408
Synchronizing a document set ...................................................................... 409
Submitting documents to CIS server .......................................................... 410
Submitting one document to CIS server ..................................................... 410
Assigning a document manually ................................................................. 411
Managing analysis results .......................................................................... 411
Test processing and production processing .................................................. 412
Switching from production view to test view ............................................... 412
Reviewing candidate documents .................................................................. 413
Analysis results .......................................................................................... 414
Category assignments .................................................................................. 414
Clearing category assignments for a taxonomy or category ......................... 415
Clearing analysis results for a document .................................................... 415
Clearing category assignments for a document .......................................... 416

Chapter 16 Resource Management ............................................................... 417
Understanding Resource Management ......................................................... 417
Managing resource agents .......................................................................... 417
Adding resource agents or modifying agent properties ............................... 418
Adding resource agents ............................................................................. 418
Viewing or modifying resource agent properties ........................................ 419
Resource agent authentication failure ......................................................... 419
Deleting resource agents ............................................................................ 419
Managing resource properties .................................................................... 420
Managing general information for resources .............................................. 421
Managing resource attributes .................................................................... 421
Managing resource operations ................................................................... 422
Starting operations ...................................................................................... 422
Viewing resource notifications ................................................................... 423
Viewing the Notification page ..................................................................... 423
Viewing resource logs ................................................................................ 424
Monitoring resources ................................................................................ 425
Manual configuration steps for monitoring resources ................................... 426

Chapter 17 Administrator Access ................................................................. 429
Administrator access sets ............................................................................ 429
Creating, viewing, or modifying administrator access sets ......................... 430
Deleting administrator access sets ............................................................... 432

Chapter 18 Client Rights Management ......................................................... 433
Client rights domains and privileged clients ............................................... 433
Client rights domains .................................................................................. 433
Creating a client rights domain ................................................................... 434
Enabling or disabling a client rights domain .............................................. 434
Deleting a client rights domain .................................................................... 434
Adding member repositories ....................................................................... 435
Viewing repository memberships ............................................................... 435
Removing a member repository from a client rights domain ...................... 436
Privileged clients ....................................................................................... 437
Adding privileged DFC clients ..................................................................... 437
Configuring privileged client trusted login and trusted server privileges ...... 438
Approving or denying privileged clients ....................................................... 439
Chapter 19  Workflow Calendars .................................................. 441
Creating a calendar .......................................................... 441
Editing a calendar ............................................................ 443
Deleting a calendar ........................................................... 443

Chapter 20  Administering Business Processes ............................. 445
Introduction to process management .................................... 446
Finding process templates .................................................. 446
Viewing process template properties search results ............... 447
Managing process templates .............................................. 448
Managing process parameters ............................................ 448
Starting a process ........................................................... 449
Viewing process instances ................................................ 449
Administering process instances ........................................ 449
Using the default process instance search page .................... 450
Performing administrative functions for an instance .............. 451
Administering tasks .......................................................... 451
Managing task details ....................................................... 453

Chapter 21  Cabinets, Files, and Virtual Documents ..................... 455
Creating cabinets ............................................................. 455
Creating folders .................................................................. 457
Creating files ...................................................................... 457
Creating a form ................................................................... 458
Working with files ............................................................. 459
Checking out files ............................................................. 459
Checking in files ............................................................... 459
Viewing checked-out files .................................................. 461
Canceling checkout ........................................................... 461
Versioning ......................................................................... 461
Moving files ....................................................................... 462
Copying files ...................................................................... 463
Viewing files in read-only mode ........................................... 463
Importing folders and files .................................................. 463
Exporting folders and files .................................................. 464
Linking cabinets, folders, or files ....................................... 465
Viewing all linked locations for an item ............................... 466
Bookmarking a document or folder ..................................... 466
Sending a link in an email message ..................................... 467
Viewing the clipboard ........................................................ 467
Deleting cabinets, folders, or files ...................................... 467
Managing subscriptions ..................................................... 467
Enabling change notifications ............................................. 468
Managing relationships ....................................................... 468
Renditions and transformations .......................................... 469
Viewing file renditions ...................................................... 469
Importing a rendition ......................................................... 469
Setting a default rendition for an object ............................... 470
Transforming a document to PDF or HTML format ............... 470
Enabling inbox notification .................................................. 470
Configuring PDF Annotation Service .......................................................... 471
Virtual documents ....................................................................................... 471
Creating a virtual document ........................................................................ 471
Viewing the structure of a virtual document ................................................. 472
Viewing virtual document content .............................................................. 473
Assembling a virtual document .................................................................. 473
Processing the SELECT statement .............................................................. 474
Setting a version label for a virtual document .............................................. 475
Creating a virtual document archive ........................................................... 475
Converting a virtual document to a simple document ............................... 476
Setting virtual document preferences ......................................................... 477
Obtaining information about virtual documents .......................................... 478
  Querying virtual documents ................................................................... 478
  Obtaining a path to a particular component ............................................. 479
    The path_name property .................................................................. 479
    Using DFC ................................................................................... 479
Email messages ............................................................................................ 480

Chapter 22  Inbox ......................................................................................... 481
Inboxes ......................................................................................................... 481
Opening a task or notification ................................................................. 482
Performing a task .................................................................................... 482
Completing a task ................................................................................... 482
Accepting a group task ............................................................................ 483
Rejecting a task ...................................................................................... 483
Delegating a task .................................................................................... 484
Repeating a task ..................................................................................... 484
Changing availability for tasks ................................................................. 484
Work queue tasks .................................................................................... 485

Chapter 23  Search ....................................................................................... 487
Searches .................................................................................................... 487
Setting search preferences ....................................................................... 487
Search guidelines ..................................................................................... 488
Running a simple search .......................................................................... 489
  Further define search terms ................................................................. 489
Running an advanced search .................................................................... 492
  Entering values for an advanced search ................................................ 492
Viewing search results ............................................................................ 495
  Smart navigation ................................................................................ 496
  Monitoring search results in real time .................................................. 496
Saving search results from external sources .......................................... 497
Additional configuration options .............................................................. 498
Saved searches ....................................................................................... 499
  Saving a search .................................................................................. 499
  Running a saved search ................................................................. 500
  Editing a saved search .................................................................. 500
Creating a search template ........................................................................ 500

Chapter 24  Tools ......................................................................................... 503
The Tools menu ........................................................................................................ 503
API and DQL ........................................................................................................... 503
Lifecycles .................................................................................................................. 503
  Assigning a lifecycle to a file .............................................................................. 504
  Removing a lifecycle from a file ......................................................................... 504
  Promoting a file to the next lifecycle state ....................................................... 504
  Demoting a file to its previous lifecycle state .................................................. 504
  Suspending a file from its current lifecycle state ............................................. 505
  Resuming a suspended file ................................................................................. 505
Workflows ............................................................................................................... 505
  Starting a workflow ............................................................................................ 505
  Sending a quickflow ........................................................................................... 507
  Viewing workflows ............................................................................................. 507
  Pausing a workflow ............................................................................................. 508
  Resuming a paused workflow ........................................................................... 508
  Stopping a workflow .......................................................................................... 508
  Emailing the workflow supervisor or a workflow performer ....................... 509
  Process a failed task in a workflow ................................................................... 509
  Changing the workflow supervisor .................................................................. 509
  Saving workflow information as a Microsoft Excel spreadsheet ............... 510
  Viewing aggregated report for workflow performance ................................ 510
  Creating a workflow template .......................................................................... 511
  Configuring the workflow agent ....................................................................... 511
    Changing the number of worker sessions ....................................................... 511
    Changing the sleep interval ........................................................................... 511
    Changing the system shutdown timeout ....................................................... 511
    Enabling immediate processing of automatic activities .............................. 512
    Tracing the workflow agent ........................................................................... 512
    Disabling the workflow agent ........................................................................ 513
Work queue management ...................................................................................... 513
  Setting up a new work queue ........................................................................... 514
  Setting up work assignment matching .......................................................... 514
    Setting up skill profiles in the process template ......................................... 515
    Defining work assignment matching filters ............................................... 515
    Adding work assignment matching filters to a work queue .................... 516
    Work queue policies ....................................................................................... 517
    Priorities of tasks ............................................................................................ 517
      Set dynamic priority and aging logic for tasks ......................................... 518
    Creating or modify a queue policy ................................................................ 518
    Defining a queue category ............................................................................. 520
    Defining a work queue .................................................................................... 520
    Defining work queue override policies ....................................................... 522
    Managing work queue users ........................................................................... 523
      Adding a user or group to a work queue ..................................................... 523
      Removing a user or group from a work queue .......................................... 524
      Adding skills to work assignment processor profiles ................................ 524
      Updating the processor profile in a work queue ....................................... 526
    Monitoring work queues ............................................................................... 527
      Assigning a work queue task to a specific user ......................................... 528
      Unassigning a work queue task from a user ............................................. 528
      Moving a work queue task to another work queue .................................. 529
      Suspending a work queue task ................................................................... 529
      Unsuspending a work queue task ............................................................... 529
      Enabling users to select tasks from the queue ......................................... 530
    Creating business calendars ......................................................................... 530
DQL Editor ............................................................................................................. 532
API Tester .............................................................................................................. 532
Chapter 25  Content Services for SAP Web Administrator ........................................ 535
SAP Web Administrator ....................................................................................... 535
Configuring Connections to SAP ....................................................................... 536
Creating, viewing, and editing connections to an SAP server ....................... 536
Creating, viewing, and editing an SAP user.................................................... 537
Configuring HTTP Archiving Services .............................................................. 537
Configuring, viewing, and editing archives ...................................................... 538
Configuring HTTP certificates for archive linking ......................................... 539
Configuring HTTP repositories for archive linking ........................................ 540
The Agent Component ...................................................................................... 540
Using Auto Manage to execute CS SAP actions .............................................. 541
Creating, viewing, and editing an Agent ......................................................... 541
Registering an HVP worker ............................................................................. 542
Creating, viewing, and editing SAP jobs ......................................................... 542
Performing job maintenance ......................................................................... 544
SAP queries ....................................................................................................... 544
Documentum queries ....................................................................................... 546
Creating, viewing, and editing a Documentum query .................................... 546
Checking the integrity of linked documents ..................................................... 546
Configuring the Manage and View Components ............................................ 547
Configuring the Manage component ............................................................... 548
Configuring the View component ................................................................... 549

Chapter 26  My Documentum for Microsoft Outlook Administration ............... 551
My Documentum for Microsoft Outlook .......................................................... 551
Overview page .................................................................................................. 552
Profiles ............................................................................................................. 553
Creating profiles .............................................................................................. 553
The Info tab ...................................................................................................... 554
The Target tab .................................................................................................. 554
The Import tab ................................................................................................. 554
The Permissions tab ....................................................................................... 556
Modifying a profile ......................................................................................... 556
Deleting profiles ............................................................................................. 556
Client Setup ..................................................................................................... 557

Chapter 27  Documentum Reporting Services ................................................... 559

Appendix A  AMP and Usage Tracking ............................................................... 561
Asset management and planning tool .............................................................. 561
Connecting to AMP .......................................................................................... 561
Required information ....................................................................................... 561
Configuring AMP to collect usage information ............................................. 562
Usage Tracking ................................................................................................ 562
Tracking internal user accounts ..................................................................... 562
Tracking unique users .................................................................................... 563
Tracking login times ...................................................................................... 563
Usage tracking and software compliance ....................................................... 564
List of Figures

Figure 1. System Information page ............................................................... 27
Figure 2. New BOCS Server Configuration - Security page .............................. 127
Figure 3. Real-time results in the search monitor screen ................................ 497
Figure 4. Content Services for SAP in Documentum Administrator .................... 535
Figure 5. Agent services .................................................................................. 541
Figure 6. Integrity checking ............................................................................ 547
Figure 7. MyDocumentum for Outlook node location in Documentum Administrator ................................................................. 552
Figure 8. The My Documentum for Microsoft Outlook Overview panel in Documentum Administrator ...................................................................................... 553
Figure 9. The Client Setup page ...................................................................... 557
# List of Tables

<table>
<thead>
<tr>
<th>Table</th>
<th>Description</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Table 1.</td>
<td>System Information page</td>
<td>27</td>
</tr>
<tr>
<td>Table 2.</td>
<td>Information on Repository page</td>
<td>33</td>
</tr>
<tr>
<td>Table 3.</td>
<td>Repository Configuration Properties</td>
<td>34</td>
</tr>
<tr>
<td>Table 4.</td>
<td>Synchronization properties</td>
<td>40</td>
</tr>
<tr>
<td>Table 5.</td>
<td>Default users created during repository configuration</td>
<td>43</td>
</tr>
<tr>
<td>Table 6.</td>
<td>Default groups created during repository configuration</td>
<td>44</td>
</tr>
<tr>
<td>Table 7.</td>
<td>Server configuration object information</td>
<td>67</td>
</tr>
<tr>
<td>Table 8.</td>
<td>Server Configuration properties tabs</td>
<td>68</td>
</tr>
<tr>
<td>Table 9.</td>
<td>General server configuration properties</td>
<td>70</td>
</tr>
<tr>
<td>Table 10.</td>
<td>Projection target information</td>
<td>76</td>
</tr>
<tr>
<td>Table 11.</td>
<td>Application server properties</td>
<td>78</td>
</tr>
<tr>
<td>Table 12.</td>
<td>Locations page properties</td>
<td>79</td>
</tr>
<tr>
<td>Table 13.</td>
<td>Federation properties</td>
<td>87</td>
</tr>
<tr>
<td>Table 14.</td>
<td>Java method server information</td>
<td>91</td>
</tr>
<tr>
<td>Table 15.</td>
<td>JMS configuration information</td>
<td>91</td>
</tr>
<tr>
<td>Table 16.</td>
<td>Associated Content Servers information</td>
<td>93</td>
</tr>
<tr>
<td>Table 17.</td>
<td>Active Java method server information</td>
<td>94</td>
</tr>
<tr>
<td>Table 18.</td>
<td>LDAP Server Configuration page properties</td>
<td>96</td>
</tr>
<tr>
<td>Table 19.</td>
<td>LDAP Server Configuration Properties properties</td>
<td>97</td>
</tr>
<tr>
<td>Table 20.</td>
<td>LDAP Server Sync &amp; Authentication properties</td>
<td>100</td>
</tr>
<tr>
<td>Table 21.</td>
<td>LDAP Server mapping properties</td>
<td>101</td>
</tr>
<tr>
<td>Table 22.</td>
<td>LDAP Server failover properties</td>
<td>103</td>
</tr>
<tr>
<td>Table 23.</td>
<td>Netscape iPlanet, Oracle Internet Directory Server, and Microsoft Active Directory example</td>
<td>105</td>
</tr>
<tr>
<td>Table 24.</td>
<td>Secondary LDAP Server page properties</td>
<td>106</td>
</tr>
<tr>
<td>Table 25.</td>
<td>Network location properties</td>
<td>114</td>
</tr>
<tr>
<td>Table 26.</td>
<td>ACS Server Configurations</td>
<td>117</td>
</tr>
<tr>
<td>Table 27.</td>
<td>ACS Server Configuration properties</td>
<td>119</td>
</tr>
<tr>
<td>Table 28.</td>
<td>ACS Projections &amp; Stores properties</td>
<td>120</td>
</tr>
<tr>
<td>Table 29.</td>
<td>ACS Connection Broker Projections properties</td>
<td>122</td>
</tr>
<tr>
<td>Table 30.</td>
<td>BOCS server properties</td>
<td>124</td>
</tr>
<tr>
<td>Table 31.</td>
<td>BOCS server security properties</td>
<td>127</td>
</tr>
<tr>
<td>Table 32.</td>
<td>Users, groups, roles, and sessions</td>
<td>133</td>
</tr>
<tr>
<td>Table 33.</td>
<td>User search filters</td>
<td>135</td>
</tr>
<tr>
<td>Table 34.</td>
<td>User properties</td>
<td>136</td>
</tr>
<tr>
<td>Table 35.</td>
<td>Import user properties</td>
<td>141</td>
</tr>
<tr>
<td>Table 36.</td>
<td>Default values for new users</td>
<td>144</td>
</tr>
<tr>
<td>Table</td>
<td>Description</td>
<td>Page</td>
</tr>
<tr>
<td>-------</td>
<td>-------------</td>
<td>------</td>
</tr>
<tr>
<td>Table 37.</td>
<td>Privileges for creating or modifying groups</td>
<td>148</td>
</tr>
<tr>
<td>Table 38.</td>
<td>Privileged groups</td>
<td>150</td>
</tr>
<tr>
<td>Table 39.</td>
<td>Group properties</td>
<td>152</td>
</tr>
<tr>
<td>Table 40.</td>
<td>Role properties</td>
<td>156</td>
</tr>
<tr>
<td>Table 41.</td>
<td>Module role properties</td>
<td>159</td>
</tr>
<tr>
<td>Table 42.</td>
<td>Session information</td>
<td>162</td>
</tr>
<tr>
<td>Table 43.</td>
<td>Permissions Sets page</td>
<td>165</td>
</tr>
<tr>
<td>Table 44.</td>
<td>Permission set properties</td>
<td>166</td>
</tr>
<tr>
<td>Table 45.</td>
<td>Permission properties</td>
<td>167</td>
</tr>
<tr>
<td>Table 46.</td>
<td>Object auditing properties</td>
<td>177</td>
</tr>
<tr>
<td>Table 47.</td>
<td>Object instance auditing properties</td>
<td>179</td>
</tr>
<tr>
<td>Table 48.</td>
<td>Audit search properties</td>
<td>180</td>
</tr>
<tr>
<td>Table 49.</td>
<td>Audit Policies page information</td>
<td>181</td>
</tr>
<tr>
<td>Table 50.</td>
<td>Audit policy information</td>
<td>182</td>
</tr>
<tr>
<td>Table 51.</td>
<td>Audit policy example values</td>
<td>183</td>
</tr>
<tr>
<td>Table 52.</td>
<td>Object and object instance auditing properties</td>
<td>183</td>
</tr>
<tr>
<td>Table 53.</td>
<td>dm_AuditMgt arguments</td>
<td>190</td>
</tr>
<tr>
<td>Table 54.</td>
<td>Logs deleted by log purge job</td>
<td>196</td>
</tr>
<tr>
<td>Table 55.</td>
<td>Job Info properties</td>
<td>202</td>
</tr>
<tr>
<td>Table 56.</td>
<td>Job Schedule properties</td>
<td>204</td>
</tr>
<tr>
<td>Table 57.</td>
<td>Job method properties</td>
<td>206</td>
</tr>
<tr>
<td>Table 58.</td>
<td>SysObject properties</td>
<td>207</td>
</tr>
<tr>
<td>Table 59.</td>
<td>Replication options</td>
<td>211</td>
</tr>
<tr>
<td>Table 60.</td>
<td>Security mode behavior</td>
<td>214</td>
</tr>
<tr>
<td>Table 61.</td>
<td>Caching rules properties</td>
<td>220</td>
</tr>
<tr>
<td>Table 62.</td>
<td>Job Connection Info properties</td>
<td>223</td>
</tr>
<tr>
<td>Table 63.</td>
<td>Method Info tab properties</td>
<td>229</td>
</tr>
<tr>
<td>Table 64.</td>
<td>SysObject Info tab properties</td>
<td>231</td>
</tr>
<tr>
<td>Table 65.</td>
<td>Parameters for moving a single object</td>
<td>243</td>
</tr>
<tr>
<td>Table 66.</td>
<td>Parameters for moving all content in a store</td>
<td>245</td>
</tr>
<tr>
<td>Table 67.</td>
<td>Parameters for moving content selected by a query</td>
<td>246</td>
</tr>
<tr>
<td>Table 68.</td>
<td>GENERATE_PARTITION_SCHEMA_SQL parameters</td>
<td>253</td>
</tr>
<tr>
<td>Table 69.</td>
<td>Alias set properties</td>
<td>268</td>
</tr>
<tr>
<td>Table 70.</td>
<td>Alias properties</td>
<td>269</td>
</tr>
<tr>
<td>Table 71.</td>
<td>Format properties</td>
<td>272</td>
</tr>
<tr>
<td>Table 72.</td>
<td>Type properties</td>
<td>276</td>
</tr>
<tr>
<td>Table 73.</td>
<td>Repository storage objects</td>
<td>286</td>
</tr>
<tr>
<td>Table 74.</td>
<td>File store properties</td>
<td>288</td>
</tr>
<tr>
<td>Table 75.</td>
<td>Linked store properties</td>
<td>293</td>
</tr>
<tr>
<td>Table 76.</td>
<td>Blob store properties</td>
<td>295</td>
</tr>
<tr>
<td>Table 77.</td>
<td>Distributed store properties</td>
<td>296</td>
</tr>
<tr>
<td>Table 78.</td>
<td>External store properties</td>
<td>299</td>
</tr>
<tr>
<td>Table 79.</td>
<td>EMC Centera store properties</td>
<td>301</td>
</tr>
</tbody>
</table>
Table of Contents

Table 80. NetApp SnapLock store properties ................................................................. 306
Table 81. Atmos store properties ..................................................................................... 309
Table 82. VIPR store properties ...................................................................................... 311
Table 83. Mount point properties .................................................................................... 312
Table 84. Location object properties ............................................................................... 313
Table 85. Plug-in properties .......................................................................................... 315
Table 86. Assignment policy properties ......................................................................... 319
Table 87. Migration policy Info tab properties ............................................................... 323
Table 88. Migration policy Schedule tab properties ....................................................... 324
Table 89. Migration policy Rules tab properties .............................................................. 324
Table 90. Migration policy SysObject tab properties ...................................................... 326
Table 91. Content delivery configuration information .................................................... 330
Table 92. Content delivery properties ............................................................................ 332
Table 93. Advanced properties for content delivery ...................................................... 334
Table 94. Content delivery replication properties ........................................................... 338
Table 95. Extra arguments ............................................................................................. 340
Table 96. Using effective labels ..................................................................................... 358
Table 97. Views for categories in Documentum Administrator ......................................... 387
Table 98. Confidence values for evidence terms ............................................................. 388
Table 99. Taxonomy settings .......................................................................................... 394
Table 100. Taxonomy settings ......................................................................................... 396
Table 101. Date formats for property rules ..................................................................... 398
Table 102. Document Set Builder settings ..................................................................... 407
Table 103. Document Set Scheduling settings ............................................................... 409
Table 104. Start Operation page properties ................................................................... 423
Table 105. Fields on the Notification page ..................................................................... 424
Table 106. Administrator access set properties .............................................................. 430
Table 107. Member repository properties ...................................................................... 435
Table 108. Privileged Clients page information ............................................................. 437
Table 109. Manage Clients page information ................................................................. 438
Table 110. Privileged client properties .......................................................................... 439
Table 111. Process template properties fields ............................................................... 447
Table 112. Process Instance search fields ...................................................................... 450
Table 113. Buttons on Process Instances page ............................................................... 451
Table 114. Task properties ............................................................................................ 451
Table 115. Administrative actions .................................................................................. 452
Table 116. Task properties ............................................................................................ 453
Table 117. Permissions tab for cabinets, folders, and files .............................................. 456
Table 118. Info tab for documents ............................................................................... 458
Table 119. Checkin information ...................................................................................... 460
Table 120. Properties for imported files ......................................................................... 464
Table 121. Virtual document preferences ...................................................................... 477
Table 122. Further define search terms ......................................................................... 489
<table>
<thead>
<tr>
<th>Table</th>
<th>Description</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>123</td>
<td>Common properties in an advanced search</td>
<td>493</td>
</tr>
<tr>
<td>124</td>
<td>Select a property-to-value relationship</td>
<td>494</td>
</tr>
<tr>
<td>125</td>
<td>User roles for work queues</td>
<td>513</td>
</tr>
<tr>
<td>126</td>
<td>Archive properties</td>
<td>538</td>
</tr>
<tr>
<td>127</td>
<td>Query types</td>
<td>545</td>
</tr>
<tr>
<td>128</td>
<td>Content Services Manage Type Defaults properties</td>
<td>548</td>
</tr>
<tr>
<td>129</td>
<td>Content Services View properties</td>
<td>549</td>
</tr>
<tr>
<td>130</td>
<td>Import properties</td>
<td>555</td>
</tr>
<tr>
<td>131</td>
<td>Effect of changing availability of My Documentum for Microsoft Outlook profile to disabled</td>
<td>556</td>
</tr>
<tr>
<td>132</td>
<td>Configuration options for clients</td>
<td>557</td>
</tr>
</tbody>
</table>
This guide describes how to use Documentum Administrator to administer and configure Content Server.

Intended audience

Documentum Administrator is a Web-based administration tool for most of the Content Server administration tasks.

The audience for Documentum Administrator are Content Server administrators, Content Intelligence Services (CIS) administrators and taxonomy managers, and Content Transformation Services (CTS) administrators. All Documentum Administrator users 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

Related documentation

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

- EMC Documentum Content Intelligence Services Administration Guide
- EMC Documentum Content Server Administration and Configuration Guide
- EMC Documentum xPlore Installation Guide
- EMC Documentum xPlore Administration and Development Guide
- EMC Documentum Content Server Fundamentals
- EMC Documentum Content Server Release Notes
- EMC Documentum Content Server Distributed Configuration Guide
## Revision history

<table>
<thead>
<tr>
<th>Revision Date</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>October 2016</td>
<td>Added point to Note in section 20.1</td>
</tr>
<tr>
<td>February 2015</td>
<td>Initial publication.</td>
</tr>
</tbody>
</table>
Chapter 1

Documentum Administrator

This chapter contains the following topics:

- Documentum Administrator, page 25
- The System Information page, page 27
- Determining the Documentum Administrator version, page 29

Documentum Administrator

Documentum Administrator is the primary user interface for administration tasks. Documentum Administrator is a web-based interface for monitoring, administering, configuring, and maintaining Documentum repositories from any system running a web browser.

Logging in to Documentum Administrator, page 25 provides URL and login information.

The EMC Documentum Administrator Deployment Guide provides information about installing Documentum Administrator.

Logging in to Documentum Administrator

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.

By default, a new Documentum Administrator installation only contains one user account with the user name and password of the installation owner. The installation owner account has superuser privileges. We strongly recommend adding at least one administrator account with system administrator privileges. The system administrator is typically the user who is responsible for configuring repositories, additional users, servers, and services.

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. On the Documentum Administrator Login page, enter the following information:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Login Name</td>
<td>Your login name.</td>
</tr>
<tr>
<td>Password</td>
<td>Your login password.</td>
</tr>
<tr>
<td>Repository</td>
<td>Select a repository from the list. If you change the repository, retype your password.</td>
</tr>
<tr>
<td>Locations</td>
<td>In the Location list (if available), select the location on the network from which you are accessing Documentum Administrator. The location allows you to access content from the nearest storage area in the network. Depending on your organization, this location can be a fixed value.</td>
</tr>
<tr>
<td>Remember my credentials</td>
<td>Select to have the system remember your credentials, so you do not have to type them again the next time you log in.</td>
</tr>
</tbody>
</table>

**More options**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Domain</td>
<td>If the repository is running in domain-required mode, type the domain name.</td>
</tr>
<tr>
<td>Language</td>
<td>To set the session locale to another language, select the language from the drop-down list.</td>
</tr>
<tr>
<td>Server</td>
<td>To connect to the repository using a particular server, select that server from the Server list box. The default is Any Running Server.</td>
</tr>
<tr>
<td>Additional Accessibility Options</td>
<td>Select Additional Accessibility Options on the login page to enable the accessibility options.</td>
</tr>
<tr>
<td>Change Password</td>
<td>To change your password in a repository, click Change Password, select a repository, and type your old and new passwords, then click Change Password. 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, click the Content Intelligence Configure link to change and validate your password on the CIS Configuration page.</td>
</tr>
</tbody>
</table>

4. Click Login.

The System Information page appears with information about the system. The System Information page, page 27 provides more information about the System Information page.

⚠️ **Caution:** In order to log in to Documentum Administrator and connect to a repository which is using a Content Server in dormant state, the user needs to be a member of the dm_datacenter_managers privileged group.
The System Information page

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

Figure 1. System Information page

The following table describes the information on the System Information page.

Table 1. System Information page

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>User</td>
<td>The user name under which you are connected.</td>
</tr>
<tr>
<td>Licensing</td>
<td>Click <strong>Configure</strong> to enable product licenses for:</td>
</tr>
<tr>
<td></td>
<td>• Collaboration Edition</td>
</tr>
<tr>
<td></td>
<td>• Federated Record Services</td>
</tr>
<tr>
<td></td>
<td>• Physical Records Management</td>
</tr>
<tr>
<td></td>
<td>• Records Manager</td>
</tr>
<tr>
<td></td>
<td>• Retention Policy Services</td>
</tr>
<tr>
<td>Repository</td>
<td>The repository to which you are connected.</td>
</tr>
<tr>
<td>Federation</td>
<td>The federation to which the current repository belongs, if any.</td>
</tr>
<tr>
<td>Field</td>
<td>Description</td>
</tr>
<tr>
<td>-------------------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Global Repository</td>
<td>The name of the global repository.</td>
</tr>
<tr>
<td>Dormancy Status</td>
<td>Indicates the dormancy status of repository.</td>
</tr>
<tr>
<td></td>
<td><strong>Note:</strong> The Dormancy Status label is only visible for 7.0 and later versions of repositories.</td>
</tr>
<tr>
<td>Content Storage Service</td>
<td>Indicates whether Content Storage Services is enabled.</td>
</tr>
<tr>
<td>Content Intelligence</td>
<td>Indicates whether Content Intelligence Services is enabled. If Content Intelligence Service is enabled, click <strong>Configure</strong> to access the <strong>Configuration for Content Intelligence</strong> page.</td>
</tr>
<tr>
<td>Content Server</td>
<td>The Content Server to which you are connected.</td>
</tr>
<tr>
<td>Server Version</td>
<td>The Content Server version and platform.</td>
</tr>
<tr>
<td>Trusted Mode</td>
<td>Indicates whether Trusted Content Services is enabled in the repository to which you are connected.</td>
</tr>
<tr>
<td>Dormancy Status</td>
<td>Indicates the dormancy status of Content Server.</td>
</tr>
<tr>
<td></td>
<td><strong>Note:</strong> The Dormancy Status label is only visible for 7.0 and later versions of Content Server.</td>
</tr>
<tr>
<td>Hostname</td>
<td>The host name of the Content Server to which you are connected.</td>
</tr>
<tr>
<td>Network Locations</td>
<td>The number of network locations associated with the repository.</td>
</tr>
<tr>
<td>BOCS Servers</td>
<td>The number of BOCS servers associated with the repository.</td>
</tr>
<tr>
<td>ACS Read</td>
<td>Indicates if users can read content in the repository through the ACS.</td>
</tr>
<tr>
<td>ACS Dormancy Status</td>
<td>Indicates the dormancy status of ACS server.</td>
</tr>
<tr>
<td></td>
<td><strong>Note:</strong> The Dormancy Status label is only visible for 7.0 and later versions of ACS server.</td>
</tr>
<tr>
<td>Messaging</td>
<td>Indicates whether the messaging server is enabled.</td>
</tr>
<tr>
<td>ACS Server</td>
<td>The name of the ACS server.</td>
</tr>
<tr>
<td>ACS Write</td>
<td>Indicates if users can write content to the repository through the ACS and whether the write is synchronous or asynchronous.</td>
</tr>
<tr>
<td>BOCS Pre-caching</td>
<td>Indicates if the repository is enabled to process pre-caching requests.</td>
</tr>
<tr>
<td>LDAP Servers</td>
<td>The number of enabled LDAP servers.</td>
</tr>
<tr>
<td>Enabled Servers</td>
<td>The number of disabled LDAP server.</td>
</tr>
<tr>
<td>Disabled Servers</td>
<td>The time and date the Content Server and LDAP servers were last synchronized.</td>
</tr>
</tbody>
</table>
Determining the Documentum Administrator version

From the System Information page, select File > About Documentum Administrator to determine the Documentum Administrator version to which you are connected.

Preferences

The Preferences menu in Documentum Administrator specifies default settings and favorites for the user interface display, virtual documents, repositories, search, and formats. Select Tools > Preferences to access the Preferences menu.
This chapter contains the following topics:

- Adding a connection broker for one session, page 31
- Configuring licenses, page 32
- Managing repositories, page 33
- Managing Content Servers, page 67
- Federations, page 85
- Java Method Servers, page 90
- LDAP servers, page 94
- LDAP Certificate Database Management, page 110

Adding a connection broker for one session

Documentum Administrator obtains connection information from the connection broker referenced in the dfc.properties file of the Documentum Administrator installation. You cannot modify the dfc.properties file using Documentum Administrator. If you have system administrator or superuser privileges, you can add connection brokers for an active session by storing connection broker information in a cookie. However, the repositories of that connection broker can only be accessed during the current session.

To add a connection broker for a session:

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
Configuring licenses

Certain Content Server and repository features require an additional license. Documentum Administrator provides a license configuration feature to enable licenses in existing repositories for the following features or products:

- Collaboration Edition
- Federated Record Services
- Physical Records Management
- Records Manager
- Retention Policy Services

To view which licenses are enabled:

1. Connect to Documentum Administrator.
   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 32.

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.
   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.
Tracking software usage and AMP

EMC Documentum provides an application for software usage reporting. The primary reporting tool, EMC Asset Management & Planning (AMP) is a virtual appliance that provides the ability to track deployed software assets and generate online and graphical reports based on the collected data. The AMP configuration and usage monitoring policies are completed through a browser interface. However, all data is contained behind the firewall of the customer to help prevent third-party access to the data. Additionally, a single instance of AMP has the ability to access multiple global registries to provide a collated view of software usage in the customer environment. This aggregated and confidential view into current usage trends allows optimizing capacity planning and asset management strategies. The usage reports, or raw data, provided in AMP can be exported if additional analysis, graphical reports or retention is needed.

The EMC Documentum Asset Management & Planning (AMP) User Guide provides information about obtaining, installing, and configuring AMP for Content Server and other EMC products. Appendix A, AMP and Usage Tracking provides more details about AMP.

If AMP is not installed, Content Server only provides basic report for the system administrator. Usage tracking (dm_usageReport), page 199 provides more information.

Managing repositories

The repository is configured on the Administration > Basic Configuration > Repository page in Documentum Administrator. A repository is represented by a docbase config object that defines configuration parameters, such as the name of the underlying RDBMS, security levels for the repository, and other operating configuration parameters.

Only users with superuser privileges can view or modify the docbase config object of a repository. It is not possible to use Documentum Administrator to create additional repositories or delete an existing repository. Adding another repository requires running the Content Server installer.

The Repository list page displays the following information:

<table>
<thead>
<tr>
<th>Table 2. Information on Repository page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Basic Configuration</td>
</tr>
<tr>
<td>Name</td>
</tr>
<tr>
<td>DBMS</td>
</tr>
<tr>
<td>Federation</td>
</tr>
</tbody>
</table>
### Basic Configuration

<table>
<thead>
<tr>
<th>Field label</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Effective Date</td>
<td>The effective date of the docbase configuration object. The effective date is used to manage client query caches.</td>
</tr>
<tr>
<td>Dormancy Status</td>
<td>The current dormancy status of the repository. Valid values are:</td>
</tr>
<tr>
<td></td>
<td>• Dormancy Requested</td>
</tr>
<tr>
<td></td>
<td>• Dormant</td>
</tr>
<tr>
<td></td>
<td>• Active</td>
</tr>
<tr>
<td></td>
<td>• Invalid</td>
</tr>
</tbody>
</table>

**Note:** The Dormancy Status column is only visible for 7.0 and later versions of repositories.

### Viewing or modifying the repository configuration

You can modify some, but not all, of the repository configuration values. This section describes the values that can be modified using Documentum Administrator.

**To view or modify the repository configuration:**

1. Start Documentum Administrator and connect as a superuser to the repository 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 displays.
4. Modify the values that you want to change, as described in Table 3, page 34.
5. If you are running the repository on a Linux host, you can enable Windows domain authentication.
6. Click the Synchronization tab to manage the repository synchronization with Documentum Offline Client.
   Modifying repository synchronization, page 40 provides the more information.
7. Click OK to accept the changes or Cancel to discard the modifications.

**Table 3. Repository Configuration Properties**

<table>
<thead>
<tr>
<th>Field label</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Database</td>
<td>The name of the RDBMS vendor. Read-only.</td>
</tr>
<tr>
<td>Repository ID</td>
<td>The repository ID number assigned during installation. Read-only.</td>
</tr>
</tbody>
</table>
### Basic Configuration

<table>
<thead>
<tr>
<th>Field label</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Federation</td>
<td>Specifies if the repository is a member of a federation. Read-only.</td>
</tr>
<tr>
<td>Security</td>
<td>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.</td>
</tr>
<tr>
<td>Index Store</td>
<td>The name of the tablespace or other storage area where type indexes for the repository are stored.</td>
</tr>
<tr>
<td>Partitioned</td>
<td>Indicates whether the repository is partitioned. When a repository is created or updated with partitioning enabled, the Content Server sets the flag to True.</td>
</tr>
</tbody>
</table>

The Partitioned field is:
- Not selectable or changeable.
- Available only in 6.5 repositories.

<table>
<thead>
<tr>
<th>Field label</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Crypto Mode</td>
<td>Displays the type of cryptography used by Content Server.</td>
</tr>
<tr>
<td>Crypto Key Store</td>
<td>Indicates the encryption key stored on the Content Server.</td>
</tr>
<tr>
<td>Dormancy Status</td>
<td>Indicates the dormancy status of repository.</td>
</tr>
</tbody>
</table>

**Note**: The Dormancy Status label is only visible for 7.0 and later versions of repositories.

### Update Configuration Changes

<table>
<thead>
<tr>
<th>Field label</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Re-Initialize Server</td>
<td>Select to reinitialize the server to which you are connected. This is necessary for changes to objects to take effect.</td>
</tr>
</tbody>
</table>

### Configuration Changes

<table>
<thead>
<tr>
<th>Field label</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Folder Security</td>
<td>Specifies whether folder security is enabled. Select to enable folder security. 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.</td>
</tr>
<tr>
<td>Rich Media</td>
<td>Specifies whether the server processes rich-media content. This feature only works if Media Server is installed in the repository. If you enable the Rich Media feature, you must re-initialize the server for the changes to take effect.</td>
</tr>
<tr>
<td>Workflow Packages</td>
<td>Specifies whether the object names of workflow package components are displayed. By default, the object names are displayed. Select this option to not display the object names.</td>
</tr>
<tr>
<td>Data Dictionary Locales</td>
<td>Specifies the locale of the data dictionary. The default local is en (English). Click <strong>Edit</strong> to configure a different locale. The server must be reinitialized for any changes to be visible.</td>
</tr>
<tr>
<td>Field label</td>
<td>Value</td>
</tr>
<tr>
<td>-----------------------------------</td>
<td>----------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Oldest Client Version</td>
<td>Specifies which DFC version is used for chunked XML documents. The value must be changed manually. If the field is left blank, the DFC format is compatible with client versions earlier than the current DFC version. If a particular DFC version is specified, clients running an earlier DFC version cannot access the chunked XML documents. 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.</td>
</tr>
<tr>
<td>Modifications Comment</td>
<td>This field is optional. It can be used to add a comment about any modifications made to the repository configuration.</td>
</tr>
<tr>
<td>Default Application Permit</td>
<td>The default user permission level for application-controlled objects accessed through an application that does not own the object. Valid values are:</td>
</tr>
<tr>
<td></td>
<td>• 2: Browse</td>
</tr>
<tr>
<td></td>
<td>• 3: Read</td>
</tr>
<tr>
<td></td>
<td>• 4: Relate</td>
</tr>
<tr>
<td></td>
<td>• 5: Version</td>
</tr>
<tr>
<td></td>
<td>• 6: Write</td>
</tr>
<tr>
<td></td>
<td>• 7: Delete</td>
</tr>
<tr>
<td></td>
<td>The default value is 3, Read permission.</td>
</tr>
<tr>
<td>Fulltext Install Locations</td>
<td>Specifies the Verity versions installed and their locations in pre-5.3 repositories.</td>
</tr>
<tr>
<td>Content Storage Services Enabled</td>
<td>Specifies whether Content Storage Services were enabled during Content Server installation. If the value is true, Content Storage Services are enabled.</td>
</tr>
<tr>
<td>Minimum Owner Permission</td>
<td>Specifies the minimum permission for an object owner after all ACL rules have been applied. The permission applies to the entire repository. Valid values are:</td>
</tr>
<tr>
<td></td>
<td>• Browse</td>
</tr>
<tr>
<td></td>
<td>• Read</td>
</tr>
<tr>
<td></td>
<td>• Relate</td>
</tr>
<tr>
<td></td>
<td>• Version</td>
</tr>
<tr>
<td></td>
<td>• Write</td>
</tr>
<tr>
<td></td>
<td>• Delete</td>
</tr>
<tr>
<td></td>
<td>The default value is <strong>Browse</strong>.</td>
</tr>
<tr>
<td>Field label</td>
<td>Value</td>
</tr>
<tr>
<td>-----------------------------------</td>
<td>----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Minimum Owner Extended</td>
<td>Specifies the minimum owner extended permissions for an object owner after all ACL rules have been applied. One or more extended permissions can be selected. By default, no extended permission is selected. Valid values are:</td>
</tr>
<tr>
<td>Permission</td>
<td>• Execute Procedure</td>
</tr>
<tr>
<td></td>
<td>Users with superuser privileges can change the owner of an item and run external procedures on certain types.</td>
</tr>
<tr>
<td></td>
<td>• Change Location</td>
</tr>
<tr>
<td></td>
<td>Allows the object owner to move the object in the repository.</td>
</tr>
<tr>
<td></td>
<td>• Change State</td>
</tr>
<tr>
<td></td>
<td>Allows the object owner to change the state of a lifecycle attached to the object.</td>
</tr>
<tr>
<td></td>
<td>• Change Permission</td>
</tr>
<tr>
<td></td>
<td>Allows the object owner to modify the basic permissions associated with the object.</td>
</tr>
<tr>
<td></td>
<td>• Change Ownership</td>
</tr>
<tr>
<td></td>
<td>Allows the object owner to change the object owner.</td>
</tr>
<tr>
<td></td>
<td>• Extended Delete</td>
</tr>
<tr>
<td></td>
<td>Allows the object owner to delete the object.</td>
</tr>
<tr>
<td></td>
<td>• Change Folder Links</td>
</tr>
<tr>
<td></td>
<td>Allows the object owner to link or unlink the object to a folder.</td>
</tr>
</tbody>
</table>

**Authorization Settings**

<table>
<thead>
<tr>
<th>MAC Access Protocol</th>
<th>The file-sharing software type in use for Macintosh clients. Valid values are:</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>• None</td>
</tr>
<tr>
<td></td>
<td>• NT</td>
</tr>
<tr>
<td></td>
<td>• Ushare</td>
</tr>
<tr>
<td></td>
<td>• Double</td>
</tr>
<tr>
<td></td>
<td>The default value is None.</td>
</tr>
<tr>
<td></td>
<td>If you change the value from NT, Ushare, or Double to None, existing resource forks are no longer be accessible.</td>
</tr>
<tr>
<td>Field label</td>
<td>Value</td>
</tr>
<tr>
<td>------------------------------</td>
<td>--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Authentication Protocol</td>
<td>Defines the authentication protocol used by the repository.</td>
</tr>
<tr>
<td></td>
<td>• On Windows, if set to Domain Required, it indicates that the repository is running in domain-required mode.</td>
</tr>
<tr>
<td></td>
<td>If a repository is running in domain-required mode, the login domain value in the login ticket generated for a user attempting to log in using an inline password defaults to the domain of the superuser even if the user on the login ticket belongs to a different domain. Users from a different domain must specify the their login domain name when logging into the repository.</td>
</tr>
<tr>
<td></td>
<td>If a repository is running in no-domain required mode, users can login with only their user name and inline password. It is also possible to prepend the user name with a backslash (). A backslash specifies an empty domain.</td>
</tr>
<tr>
<td></td>
<td>• On Linux platforms, choose between Linux authentication or Windows domain authentication.</td>
</tr>
<tr>
<td>Cached Query Effective Date</td>
<td>Used to manage the client query caches. The default is NULLDATE.</td>
</tr>
<tr>
<td>Run Actions As</td>
<td>The user account that is used to run business policy (document lifecycle) actions. Options are:</td>
</tr>
<tr>
<td></td>
<td>• Session User (default)</td>
</tr>
<tr>
<td></td>
<td>• Superuser</td>
</tr>
<tr>
<td></td>
<td>• Lifecycle Owner</td>
</tr>
<tr>
<td></td>
<td>• Named User</td>
</tr>
<tr>
<td></td>
<td>If selected, click the Select User link to access the Choose a user page to select a user.</td>
</tr>
<tr>
<td>Login Tickets</td>
<td>Specifies that all other repositories are trusted and login tickets from all repositories are accepted by the current repository.</td>
</tr>
<tr>
<td></td>
<td>If selected, <strong>Allow login tickets from repositories</strong> is not displayed.</td>
</tr>
<tr>
<td>Allow login tickets from</td>
<td>This field is only displayed if <strong>Allow all login tickets</strong> is not selected.</td>
</tr>
<tr>
<td>repositories</td>
<td>Click <strong>Select</strong> to access the Choose Repositories page to designate repositories whose login tickets are permitted in the current repository (the trusted repositories).</td>
</tr>
<tr>
<td>Field label</td>
<td>Value</td>
</tr>
<tr>
<td>------------------------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Designate Login Ticket Expiration</td>
<td>Specifies the earliest possible creation date for valid login tickets. Tickets issued before the designated date are not valid in the current repository. Select one of the following:</td>
</tr>
<tr>
<td></td>
<td>• Null date: Specifies that there is no cutoff date for login tickets in the current repository. This is the default value.</td>
</tr>
<tr>
<td></td>
<td>• Expire login tickets on the following date and time: Specifies the earliest possible creation date for valid login tickets. Use the calendar control to choose the correct date and time.</td>
</tr>
<tr>
<td></td>
<td>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.</td>
</tr>
<tr>
<td>Maximum Authentication Attempts</td>
<td>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.</td>
</tr>
<tr>
<td></td>
<td>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.</td>
</tr>
<tr>
<td></td>
<td>A value of zero (0) means that the feature is not enabled.</td>
</tr>
<tr>
<td></td>
<td>Requires the server to be reinitialized for changes to take effect.</td>
</tr>
<tr>
<td>LDAP Synchronization On-Demand</td>
<td>Used to synchronize LDAP directory users with the repository between scheduled runs of the LDAP synchronization job:</td>
</tr>
<tr>
<td></td>
<td>• When cleared, LDAP directory users who do not exist in the repository cannot log in.</td>
</tr>
<tr>
<td></td>
<td>• 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.</td>
</tr>
<tr>
<td>Privileged Clients</td>
<td>Boolean. If selected, indicates that the repository is accessible to privileged clients only.</td>
</tr>
<tr>
<td></td>
<td>This checkbox is only available if a DFC client exists in the repository and is approved to perform privilege escalations.</td>
</tr>
</tbody>
</table>
Modifying repository synchronization

The synchronization options control the behavior of Documentum Offline Client.

**To modify the synchronization settings for a repository:**

1. Connect as a superuser to the repository for which you want to modify synchronization with Documentum Offline Client.
2. Navigate to Administration > Basic Configuration > Repository to access the Repository list page.
3. Select the repository name, 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, as described in Table 4, page 40.
6. Click OK to accept the changes.

**Table 4. Synchronization properties**

<table>
<thead>
<tr>
<th>Field label</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Synchronization Settings</td>
<td>For repositories where Offline Client is enabled. Options are:</td>
</tr>
<tr>
<td></td>
<td>• None: no content synchronization to local machine.</td>
</tr>
<tr>
<td></td>
<td>No content is synchronized to the local machine.  This is the default setting for a repository.</td>
</tr>
<tr>
<td></td>
<td>• Basic: 1-way download to local machine as read only.</td>
</tr>
<tr>
<td></td>
<td>Content is downloaded to the local machine and marked read-only. No content is uploaded from the local machine.</td>
</tr>
<tr>
<td></td>
<td>• Role-Based: assign sync permissions to specific repository roles.</td>
</tr>
<tr>
<td></td>
<td>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.</td>
</tr>
<tr>
<td>Field label</td>
<td>Value</td>
</tr>
<tr>
<td>---------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Synchronization Role</td>
<td>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 Chose a user/group page to select users who you want to use offline upload.</td>
</tr>
<tr>
<td>Check In Settings</td>
<td>Select to use the client dialog or the user’s local settings to check content into the repository. Options are:</td>
</tr>
<tr>
<td></td>
<td>• Always Use client dialog to check in content</td>
</tr>
<tr>
<td></td>
<td>• Use User’s local check in setting</td>
</tr>
</tbody>
</table>

### Moving a repository to dormant and active states

This section describes how to move a repository to a dormant state and back to an active state.

A repository can be moved to a dormant state only from an active state. To perform this operation, you should be a member of the dm_datacenter_managers, a privileged group whose membership is maintained by superusers. This feature is only applicable for 7.0 and later versions of repositories.

**To move a repository to a dormant state:**

1. Navigate to Administration > Basic Configuration > Repository. The Repository list page appears.
2. Select a repository that needs to be made dormant.
3. On the Repository page, do one of the following:
   - Select a repository in the Name column, then select Tools > Make Dormant.
   - Select a repository in the Name column and then right-click. From the available menu options, select Make Dormant.
4. In the confirmation page, click OK to confirm with the request to move a repository to a dormant state or Cancel to exit.

When you click OK, the Repository page displays.

The system displays the message Repository moved to dormant state successfully.

**Note:**

- When a repository is moved to a dormant state, the status of all the Content Servers and ACS servers for this repository will also be moved to a dormant state.
- In a multiple Content Server setup, moving a repository to a dormant state will move all the configured Content Servers to a dormant state. However, there will be delay in moving the non-connected servers to a dormant state. This delay is equal to the value of database_refresh_interval key as specified in server.ini. The database_refresh_interval key
defines how often the main server thread (parent server) reads the repository to refresh its global caches. You can raise this value but it cannot be lowered. The default value is 1 minute.

- For a WDK application to login to a repository in a dormant state, dmc_wdk_presets_owner, dmc_wdk_preferences_owner, and dm_bof_registry users should be a member of dm_datacenter_managers.

A repository can be moved back to an active state only from a dormant state. To perform this operation, you should be a member of the dm_datacenter_managers, a privileged group whose membership is maintained by superusers. This feature is only applicable for 7.0 and later versions of repositories.

**To move a repository to an active state:**

1. Navigate to Administration > Basic Configuration > Repository.
   The Repository list page appears.
2. Select a repository that needs to be made active.
3. On the Repository page, do one of the following:
   - Select a repository in the Name column, then select Tools > Make Active.
   - Select a repository in the Name column and then right-click. From the available menu options, select Make Active.
4. In the confirmation page, click OK to confirm with the request to move a repository to an active state or Cancel to exit.

When you click OK, the Repository page displays.
The system displays the message **Repository moved to active state successfully.**

**Note:** When a repository is moved to an active state, the status of all the Content Servers and ACS servers for this repository will also be moved to an active state.

---

**Enabling a repository as a global registry**

Enabling a repository as a global registry after configuration, requires activating the dm_bof_registry user. The global registry and user credentials can also be configured in the dfc.properties file.

**To enable a repository as a global registry:**

1. Open Documentum Administrator and connect to the repository.
2. Navigate to Administration > User Management > Users.
3. Locate the dm_bof_registry user and select View > Properties > Info to access the User Properties page.
4. Verify that the Name value is dm_bof_registry.
   The dm_bof_registry Name value is required, but you have the option to change the User Login Name value, if desired.
5. Change the password.
6. Activate the user by selecting Active from the State drop-down list.
7. Click OK to save your changes.
During the DFC installation on client machines, such as the Documentum Administrator host, provide the user login name and password for the dm_bof_registry user. This action updates the dfc.properties file and enables the DFC installation to contact the global registry.

To modify the dfc.properties file manually:
1. On the DFC host, navigate to $DOCUMENTUM/config (Linux) or %DOCUMENTUM%\config (Windows).
2. From a command prompt, execute the following command to generate the encrypted form of the global registry user’s password:
   
   ```
   java -cp dfc.jar com.documentum.fc.tools.RegistryPasswordUtils password_of_user
   
   where password_of_user is the clear-text password of the global registry user.
   
   3. Open the dfc.properties file in a text editor and modify the following attributes:
   
   ```
   dfc.globalregistry.repository=global_registry_repository_name
   dfc.globalregistry.username=user_login_name
   dfc.globalregistry.password=encrypted_password_of_user
   
   where encrypted_password_of_user is the encrypted password you generated in step 2.
   ```

   4. Save the dfc.properties file.

Repository content

The Content Server installation program and the scripts that run during repository configuration automatically create various objects, such as cabinets, configuration objects, users, and groups.

Table 5, page 43 lists the default users that are created during repository configuration.

Table 5. Default users created during repository configuration

<table>
<thead>
<tr>
<th>User</th>
<th>User Privileges</th>
<th>Extended User Privileges</th>
</tr>
</thead>
<tbody>
<tr>
<td>repository_owner</td>
<td>Superuser</td>
<td>None</td>
</tr>
<tr>
<td>installation_owner</td>
<td>Superuser</td>
<td>None</td>
</tr>
<tr>
<td>global registry user</td>
<td>None</td>
<td>None</td>
</tr>
<tr>
<td>dm_bpm_inbound_user</td>
<td>None</td>
<td>None</td>
</tr>
<tr>
<td>dm_autorender_win32</td>
<td>System Administrator</td>
<td>None</td>
</tr>
<tr>
<td>dm_autorender_mac</td>
<td>System Administrator</td>
<td>None</td>
</tr>
<tr>
<td>dm_mediaserver</td>
<td>System Administrator</td>
<td>None</td>
</tr>
<tr>
<td>dm_fulltext_index_user</td>
<td>Superuser</td>
<td>None</td>
</tr>
</tbody>
</table>

The configuration program creates a number of default groups. Table 6, page 44 describes the default groups. In addition to the default groups, the configuration program also creates a set of privileged groups. Privileged groups, page 149 provides more information about privileged groups.
Table 6. Default groups created during repository configuration

<table>
<thead>
<tr>
<th>Group</th>
<th>Members</th>
</tr>
</thead>
<tbody>
<tr>
<td>admingroup</td>
<td>installation_owner, repository_owner</td>
</tr>
<tr>
<td>docu</td>
<td>repository_owner, installation_owner,</td>
</tr>
<tr>
<td></td>
<td>dm_autorender_win32, dm_autorender_mac,</td>
</tr>
<tr>
<td></td>
<td>dm_mediaserver</td>
</tr>
<tr>
<td>queue_admin</td>
<td>None.</td>
</tr>
<tr>
<td></td>
<td>This is a role group supporting the queue</td>
</tr>
<tr>
<td></td>
<td>management feature of Documentum Process</td>
</tr>
<tr>
<td></td>
<td>Builder.</td>
</tr>
<tr>
<td>queue_manager</td>
<td>queue_admin group</td>
</tr>
<tr>
<td></td>
<td>This is a role group supporting the queue</td>
</tr>
<tr>
<td></td>
<td>management feature of Documentum Process</td>
</tr>
<tr>
<td></td>
<td>Builder.</td>
</tr>
<tr>
<td>queue_processor</td>
<td>queue_manager group</td>
</tr>
<tr>
<td></td>
<td>This is a role group supporting the queue</td>
</tr>
<tr>
<td></td>
<td>management feature of Documentum Process</td>
</tr>
<tr>
<td></td>
<td>Builder.</td>
</tr>
<tr>
<td>process_report_admin</td>
<td>queue_admin</td>
</tr>
<tr>
<td></td>
<td>This is a role group supporting the queue</td>
</tr>
<tr>
<td></td>
<td>management feature of Documentum Process</td>
</tr>
<tr>
<td></td>
<td>Builder.</td>
</tr>
</tbody>
</table>

Type indexes

Indexes on the object type tables in the RDBMS enhance the performance of repository queries. When a repository is configured, the Content Server creates various object type indexes. There are several administration methods for managing type indexes:

- **MAKE_INDEX**
  
  Creates type indexes for special requirements. *MAKE_INDEX, page 255* provides more information about the MAKE_INDEX method.

- **MOVE_INDEX**
  
  By default, type tables and indexes are stored in the same tablespace or segment. However, you can create a repository with separate tablespaces or segments for each or you can move the indexes later, using the MOVE_INDEX method. Indexes that you create can be placed in any directory. *MOVE_INDEX, page 256* provides more information about the MAKE_INDEX method.

  The *EMC Documentum Content Server Installation Guide* provides more information about creating a repository with separate tablespaces.

- **DROP_INDEX**
Removes a user-defined index. It is strongly recommended to not remove any of the system-defined indexes. DROP_INDEX, page 251 provides more information about the DROP_INDEX method.

Each method can be executed through Documentum Administrator, an apply method, or the DQL EXECUTE statement.

**Date values**

By default, Content Server stores date values as UTC (Coordinated Universal Time) time in new repositories (Documentum 6 and later), and as the local time in repositories that are upgraded from before version 6.

The r_normal_tz property in the docbase config object controls how Content Server stores dates in the repository. If the property value is 0, all dates are stored in UTC time. If the property contains an offset value, dates are normalized using the offset value before being stored in the repository. Offset values must use a time zone offset from UTC time, expressed as seconds. For example, if the offset represents the Pacific Standard Time zone, the offset value is -8*60*60, or -28800 seconds. When the property is set to an offset value, Content Server stores all date values based on the time identified by the time zone offset.

In a Documentum 6 or later repository, r_normal_tz value is set to 0. In a repository upgraded from a release earlier than version 6, the r_normal_tz value is set to the offset that represents Content Server local time and cannot be changed.

**Moving or duplicating a repository**

Moving or duplicating a repository requires dump and load operations. Dump and load operations can be used to:

- Move part of a repository from one location to another.
- Duplicate part of a repository.

Use dump and load operations to create a duplicated repository with a different name or repository ID than the source repository.

Dump or load operations require superuser privileges. A dump operation creates a binary file of objects dumped from a repository. If a dumped object has associated content files, the content files are either referenced by full path or included directly in the dump file. The load operation loads the objects and content files into another repository.

Dump files are created by using the session code page. For example, if the session in which the dump file was created was using UTF-8, the dump file is a UTF-8 dump file. The repository into which the dump file is loaded must use the same code page the source repository.

Dump and load operations can be performed manually using either IAPI, Docbasic scripts, or the IDfIDumpRecord and IDfLoadRecord DFC interfaces.

**Note:** Dump and load operations require additional steps for repositories where Web Publisher is installed. The *EMC Documentum Web Publisher Deployment Guide* provides the details.
Supporting object types

There are several object types that support dump and load operations:

- **Dump Record (dm_dump_record)**
  
  A dump record object contains information about a specific dump execution. It has a property that contains the name of the file with the dumped information and properties whose values tell Content Server which objects to copy into the specified file.

- **Dump Object Record (dmi_dump_object_record)**
  
  A dump object record object contains information about one specific object that is copied out to the dump file. Dump object record objects are used internally.

- **Load Record (dm_load_record)**
  
  A load record object contains information about a specific load operation. Its properties are used by Content Server to manage the loading process. It also has two properties that contain the starting and ending times of the load operation.

- **Load Object Record (dmi_load_object_record)**
  
  A load object record object contains information about one specific object that is loaded from the dump file into a repository. Load object record objects are used internally.

The *EMC Documentum System Object Reference Guide*, provides information about the properties of these object types.

Dumping objects under retention

If a dumped SysObject is associated with a retainer, the dump operation also dumps the retainer. Retainers record retention policy definitions.

If a retainer object is dumped directly, the object identified in the retainer_root_id property of the retainer is also dumped. That object can be a single SysObject or a container, such as a folder. If it is a container, the objects in that container are not dumped, only the container itself is dumped.

**Note:** This information does not apply to dump and load operations that are used to execute object replication jobs.

Aspects and dump operations

A dump operation does not dump aspects associated with a dumped object. If aspects are associated with specific instances of an object type, those aspects must be created in the target repository. Similarly, if default aspects are defined for an object type and instances of that type are dumped, the default aspects must be manually created in the target repository. The aspects must be created in the target repository before performing the load operation.
Dumping an entire repository

Dumping the contents of an entire repository by setting the dump_operation property of the dump record object to full_docbase_dump is currently not supported.

Dumping specific objects

To dump only specific objects in a repository, set the type, predicate, and predicate2 repeating properties of the dump record object. The type property identifies the type of object you want to dump and the predicate and predicate2 properties define a qualification that determines which objects of that type are dumped. The EMC Documentum System Object Reference Manual contains a full description of a dump record object's properties.

However, when you dump an object, the server includes any objects referenced by the dumped object. This process is recursive, so the resulting dump file can contain many more objects than the object specified in the type, predicate, and predicate2 repeating properties of the dump record object.

When dumping a type that has a null supertype, the server also dumps all the objects whose r_object_ids are listed in the ID field of the type.

The ACL associated with a dumped object is also dumped.

Setting the type property

The type property is a repeating property. The object type specified at each index position is associated with the WHERE clause qualification defined in the predicate at the corresponding position.

The dump operation dumps objects of the specified type and any of its subtypes that meet the qualification specified in the predicate. Consequently, it is not necessary to specify each type by name in the type property. For example, if you specify the SysObject type, then Content Server dumps objects of any SysObject or SysObject subtype that meets the qualification.

Use the following guidelines when specifying object types and predicates:

- The object type must be identified by using its internal name, such as dm_document or dmr_containment.

Object type definitions are only dumped if objects of that type are dumped or if objects that are a subtype of the type are dumped.

This means that if a subtype of a specified type has no objects in the repository or if no objects of the subtype are dumped, the dump process does not dump the subtype's definition. For example, suppose you have a subtype of documents called proposal, but there are no objects of that type in the repository yet. If you dump the repository and specify dm_document as a type to dump, the type definition of the proposal subtype is not dumped.

This behavior is important to remember if you have user-defined subtypes in the repository and want to ensure that their definitions are loaded into the target repository.

- To dump subtype definitions for types that have no objects instances in the repository or whose objects are not dumped, you must explicitly specify the subtype in the dump script.
• If you have created user-defined types that have no supertype, be sure to explicitly include them in the dump script if you want to dump objects of those types. For example, the following commands will include all instances of your_type_name:

```plaintext
append,c,l,type
your_type_name
append,c,l,predicate
l=1
```

• If you have system or private ACLs that are not currently associated with an object, they are not dumped unless you specify dm_acl as a type in the dump script. For example, include the following lines in a dump script to dump all ACLs in the repository (including orphan ACLs):

```plaintext
append,c,l,type
dm_acl
append,c,l,predicate
l=1
```

You may want to specify a qualification in the predicate to exclude orphaned internal ACLs.

• By default, storage area definitions are only included if content associated with the storage is dumped. If you want to dump the definitions of all storage areas, even though you may not dump content from some, include the storage type (file store, linked, and distributed) explicitly in the dump script.

• When you dump the dm_registered object type, Content Server dumps only the object (dm_registered) that corresponds to the registered table. The underlying RDBMS table is not dumped. Use the dump facilities of the underlying RDBMS to dump the underlying table.

### Setting the predicate properties

You must supply a predicate for each object type you define in the type property. If you fail to supply a predicate for a specified type, then no objects of that type are dumped.

To dump all instances of the type, specify a predicate that is true for all instances of the type, such as 1=1.

To dump a subset of the instances of the object type, define a WHERE clause qualification in the predicate properties. The qualification is imposed on the object type specified at the corresponding index level in the type property. That is, the qualification defined in predicate[0] is imposed on the type defined in type[0], the qualification defined in predicate[1] is imposed on the type defined in type[1], and so forth.

For example, if the value of type[1] is dm_document and the value of predicate[1] is object_name = 'foo', then only documents or document subtypes that have an object name of foo are dumped. The qualification can be any valid WHERE clause qualification. The EMC Documentum Content Server DQL Reference Manual contains the description of a valid WHERE clause qualification.

The predicate property accepts a maximum of 255 characters. If the qualification exceeds 255 characters, place the remaining characters in the predicate2 property at the corresponding index level. For example, if the qualification defined for type[0] is 300 characters, you put the first 255 characters in predicate[0] and the remaining 45 in predicate2[0]. When the dump is executed, Content Server concatenates predicate[0] and predicate2[0]. The predicate2 property accepts a maximum of 255 characters also.
**Important:** If you use the predicate2 property at any index position, you must also set the predicate2 property at all index positions before the desired position. Content Server does not allow you to skip index positions when setting repeating properties. For example, if you set predicate2[2] and predicate2[4], you must also set predicate2[0], predicate2[1], and predicate2[3]. It is valid to set the values for these intervening index positions to a single blank.

### Content files and dumping

How the dump operation handles content depends on where the content is stored and how the include_content parameter is set in the dump_parameter argument of the dump object.

By default, if the content is stored in a file store, EMC Centera storage area, or NetApp SnapLock storage area, the content is not included in the dump file. You can set the include_content parameter to include such content. If you are dumping a repository that has encrypted file store storage areas, you must include the content in the dump file. Content Server decrypts the content before placing it into the dump file.

*Dumping without content, page 49* describes the default behavior and requirements for handling dump files without content. *Including content, page 49* describes how to include content and the requirements for dump files with content.

If the content is stored in a blob or turbo storage area, the content is automatically included in the dump file because the content is stored in the repository.

Content stored in external storage cannot be included in a dump file.

### Dumping without content

By default, a dump operation on content in file stores, EMC Centera stores, or NetApp SnapLock stores does not include content. Instead, when an object with content is dumped, the operation places a reference to the content in the dump file. If the content is stored in a file system, the reference is a file system path. If the object is stored in a retention storage system, the reference is the content’s address.

When the dump file is loaded into the target repository, any file systems referenced for content must be visible to the server at the target site. For content in retention storage, the ca_store object at the target site must have an identical definition as the ca_store object at the source repository and must point to the same storage system used by the source repository.

In the target repository, the storage objects for the newly loaded content must have the same name as the storage objects in the source repository but the filepaths for the storage locations must be different.

The owner of the target repository must have Read permission in the content storage areas of the dumped repository when the load operation is executed. The load operation uses the target repository owner’s account to read the files in the source repository and copy them into the target repository.

### Including content

To include content in a dump file, set the include_content property to T (TRUE) in the dump record object. If the property is true, when Content Server dumps an object with content, the content is copied
into the dump file also. The content must be stored in a file store, EMC Centera store, or NetApp SnapLock storage area. Content Server cannot copy content from external storage into a dump file.

In the target repository, the storage objects for the newly loaded content must have the same names as those in the source repository, but the actual directory location, or IP address for a retention store, can be different or the same.

Always include content if you are dumping a repository to make a backup copy, to archive a repository, or to move the content or if the repository includes an encrypted storage area.

**Compressing content**

When you include content, you can create a compressed dump file to save space. To compress the content in the dump file, set the dump\_parameter property to compress\_content = T.

Content Server automatically decompresses a compressed dump file during a load operation.

**Setting the cache size**

Content Server uses an in-memory cache to store the object IDs of dumped objects. Before dumping an object, Content Server checks the cache to see if the object has already been dumped.

You can improve the performance of a large dump operation by setting a larger cache size. If you do not specify a cache size, the server uses a default size of 1 MB, which can hold up to 43,690 object IDs.

To increase the cache size, set the cache\_size argument of the dump\_parameter property to a value between 1 and 100. The value is interpreted as megabytes and defines the maximum cache size. The memory used for the cache is allocated dynamically as the number of dumped objects increases.

Content Server ignores the cache setting when doing a full repository dump.

**Using non-restartable dump**

You can also improve the performance of a dump operation by creating a non-restartable dump. However, if a non-restartable dump operation fails, you will not be able to restart the dump from the failure point. Instead, you must create a new dump record object to start the dump operation from the beginning.

A dump operation can only be non-restartable if it is a partial repository dump. Full repository dump operations are always restartable.

To create a non-restartable dump, set the dump\_parameter property to restartable=F.

**Using a script to create a dump file**

For dump operations that you execute regularly, we recommend that you write a script that creates and saves the dump object and checks for errors after the execution. Using a script avoids re-creating the dump object manually each time you want to perform the task.
To use a script:

1. Write a script that creates the dump object, sets its properties, saves the object, and checks for errors.
   
   If you do not set the file_name property to a full path, Content Server assumes the path is relative to the root directory of the server. The filename must be unique within its directory. This means that after a successful load operation that uses the dump file, you must move the dump file to archival storage or destroy it so you can successfully execute the script later.

2. Use IAPI to execute the script. Use the following command-line syntax:
   
   ```
iapi source_db -Username -Ppassword < script_filename
   ```
   
   where:
   - `source_db` is the name of the repository that you want to dump.
   - `username` is the user name of the user who is executing the operation.
   - `password` is the user password.
   - `script_filename` is the name of the file you created in Step 1.

3. If the dump was successful, destroy the dump object. If the Save on the dump operation did not return OK, the dump was not successful.
   
   Destruction of the dump object cleans up the repository and removes the dump object records and state information that are no longer needed.

Sample script for a partial repository dump

**Note:** There is a template for a sample script in `%DM_HOME%\install\DBA\dump_template.bat` ($DM_HOME/install/DBA/dump_template.api ).

The script below has the following characteristics:

- It does not copy content files into the dump file.
- It only dumps ACLs associated with a dumped object.
- It does not dump subtype definitions if there are no objects of that subtype.
- It does not dump storage area definitions if the dump does not include any content associated with the storage area.
- It does not dump user-defined subtypes that have no supertype.
- It does not dump job objects.
- It is not restartable.

The script assumes that you want to dump all instances of the types, not just a subset. Consequently, the predicates are set as `I=1` (you cannot leave them blank). If you want to dump only some subset of objects or want to include all ACLs, type definitions, or storage area definitions, modify the script accordingly.

Here is the script:

```
create,c,dm_dump_record
set,c,1,file_name
dump file name# Supply your own file name.
# This must be a new file
append,c,1,type
```
Basic Configuration

dm_sysobject
append,c,l,predicate
l=1
append,c,l,type
dm_assembly
append,c,l,predicate
l=1
append,c,l,type
dm_format
append,c,l,predicate
l=1
append,c,l,type
dm_user
append,c,l,predicate
l=1
append,c,l,type
dm_group
append,c,l,predicate
l=1
append,c,l,type
dmi_queue_item
append,c,l,predicate
l=1
append,c,l,type
dmi_registry
append,c,l,predicate
l=1
append,c,l,type
dm_relation
append,c,l,predicate
l=1
append,c,l,type
dm_relation_type
append,c,l,predicate
l=1
append,c,l,type
dmr_containment
append,c,l,predicate
l=1
append,c,l,type
dmr_content
append,c,l,predicate
l=1
append,c,l,dump_parameter
cache_size=60 #set cache size
append,c,l,dump_parameter
restartable=F #non-restartable dump
append,c,l,predicate
l=1
save,c,l
getmessage,c

Notes:

• In the append command line, the l is the lowercase letter L.

• If you do not set the file_name property to a full path, Content Server assumes the path is relative to the root directory of the server. The filename must be unique within its directory. This means that after a successful load operation using the dump file, you must move the dump file to archival storage or destroy it so that you can successfully execute the script later.

• To dump user-defined types that have no supertype, add Append methods for each to the script:

append,c,l,type
your_type_name
If the server crashes during a dump operation

If Content Server crashes during a dump operation, there are two alternatives:

- Destroy the dump file (target file named in the script) if it exists and then re-execute the script.
  
  If the specified file already exists when you try to save a new dump record object, the save operation fails. Re-executing the script creates a new dump record object.

- If the dump operation is restartable, fetch the existing dump object from the source repository and save it again. Saving the object starts the dump operation. Content Server begins where it left off when the crash occurred.

Moving the dump file

The dump file is a binary file. If you move a dump file from one machine to another electronically, be sure to use a binary transfer protocol.

If your operating system is configured to allow files larger than 2 GB, the dump file can exceed 2 GB in size. If you create a dump file larger than 2 GB, you cannot load it on a machine that does not support large file sizes or large file systems.

Loading a repository

Loading a repository puts the objects stored in a dump file into the repository. The dump file header does not indicate the session code page in which the dump file was created. If you do not know the session code page in use when a dump file was created, do not load the dump file.

If the dump file does not include the actual content files associated with the objects you are loading, the operation reads the content from the storage areas of the dumped repository. This means that the owner of the repository that you are loading must have Read privileges at the operating system level for the storage areas in the source repository.

The load operation generates a dmi_queue_item for the dm_save event for each object of type SysObject or a subtype that is loaded into the target repository. The event is queued to the dm_fulltext_index_user user account. This ensures that the objects are added to the target repository’s index. You can turn off this behavior. Turning off save event generation during load operations, page 54 provides the detailed instructions.

Loading a repository is accomplished by creating and saving a load record object. The act of saving the object starts the operation.

Note: The load operation performs periodic commits to the repository. Consequently, you cannot load a repository if you are in an explicit transaction. The Content Server does not allow you to save a load record object if you are in an explicit transaction. Similarly, you cannot perform a revert or destroy operation on a load record object if you are in an explicit transaction.
Refreshing repository objects from a dump file

Generally, when you load objects into a repository, the operation does not overwrite any existing objects in the repository. However, in two situations overwriting an existing object is the desired behavior:

- When replicating content between distributed storage areas
- When restoring archived content

In both situations, the content object that you are loading into the repository could already exist. To accommodate these instances, the load record object has a relocate property. The relocate property is a Boolean property that controls whether the load operation assigns new object IDs to the objects it is loading.

The type and predicate properties are for internal use and cannot be used to load documents of a certain type.

Loading job objects

If you dump and load job objects, the load operation automatically sets the job to inactive in the new repository. This ensures that the job is not unintentionally started before the load process is finished and it allows you the opportunity to modify the job object if needed. For example, to adjust the scheduling to coordinate with other jobs in the new repository.

The load operation sets jobs to inactive (is_inactive=TRUE) when it loads the jobs, and sets the jobs’ run_now property to FALSE.

If the load operation finds an existing job in the target repository that has the same name as a job it is trying to load, it does not load the job from the dump file.

Loading registered tables

When you load a registered table, the table permits defined for that table are carried over to the target repository.

Turning off save event generation during load operations

During a load operation, every object of type SysObject or SysObject subtype loaded into the target repository generates a save event. The event is queued to the dm_fulltext_index_user. This behavior ensures that the object is added to the target index of the repository.

The behavior is controlled by the load parameter called generate_event. The parameter is T by default. If you do not want the load operation to queue save events to the dm_fulltext_index_user, set the parameter to F for the operation. The parameter is set in the load_parameter property as:

```text
generate_event=F
```
Loading a new repository

New repositories are not empty. They contain various cabinets and folders created by the installation process, such as:

- A user object for the repository owner
- A cabinet for the repository owner
- The docu group
- The System cabinet, which contains a number of subfolders
- The Temp cabinet

When you load a dump file into a new repository, these objects are not replaced by their counterparts in the dump file because they already exist in the new repository.

However, if you have changed any of these objects in the source repository (the source of the dump file), the changes are lost because these objects are not loaded. For example, if you have added any users to the docu group or if you have altered permissions on the System cabinet, those changes are lost.

To ensure that any changes you have made are not lost, fetch from the source repository any of the system objects that you have altered and then use the Dump method to get a record of the changes. For example, if the repository owner’s cabinet was modified, use the following command sequence to obtain a listing of its property values:

```
fetch,c,cabinet_id
dump,c,l
```

After the load operation, you can fetch and dump the objects from the new repository, compare the new dump results with the previous dump results, and make any necessary changes.

The preLoad utility

Documentum provides a utility that you can run on a dump file to tell you what objects that you must create in the new repository before you load the dump file. The utility can also create a DQL script that you can edit and then run to create the needed objects. The syntax for the preload utility is:

```
preload repository [-Username] -Ppassword -dump_file filename
                   [-script_file name]
```

- `repository` is the name of the repository into which you are loading the dump file.
- `filename` is the name of the dump file.
- `name` defines a name for the output DQL script.

If you do not include a username, the current user is assumed.

**Note:** This utility does not report all storage areas in the source repository, but only those that have been copied into the dump file.

Load procedure for new repositories

Use the following procedure to load a dump file into a new repository.
Note: You cannot perform this procedure in an explicit transaction because the load operation performs periodic commits to the repository. Content Server does not allow you to save the load record object to start the load operation if you are in an explicit transaction.

To load a dump file into a new repository:

1. Create the repository.
   
   Notes:
   - If the repository shares any directories with the source repository, you must assign the repository an ID that differs from the source repository ID.
   - If the old and new repositories have different owners, ensure that the new repository's owner has Read privileges in the storage areas used by the old repository if the old repository was not dumped with the include_content property set to TRUE.

2. Create the necessary storage objects and associated location objects in your new repository.
   
   Each storage object in your source repository must have a storage object with the same name in the new repository. The filestore objects in the new repository must reference location objects that point to actual directories that differ from those referenced by the location objects in the source repository.
   
   For example, suppose you have a file store object with the name storage_1 in your source repository that points to the location object named engr_store, which references the d:\documentum\data\engr (/u04/home/installation_owner/data/engr) directory. In the new repository, you must create a file store object with the name storage_1 that references a location object that points to a different directory.
   
   Note: The location objects can be named with different names or they can have the same name. Either option is acceptable.

3. If your storage areas in the source repository had associated full-text indexes, create corresponding full-text index objects and their location objects in the new repository. Note that these have the same naming requirements as the new storage objects described in Load procedure for new repositories, page 55.

4. Create and save the following script:

   ```plaintext
   create,c,dm_load_record
   set,c,1,file_name
   full_path_of_dump_file
   save,c,1
   getmessage,c
   ```

5. Log in as the owner of the installation and use IAPI to execute the script.

   When you start IAPI, connect to the new repository as a user who has Sysadmin privileges in the repository.

6. After the load completes successfully, you can destroy the load object:

   ```plaintext
   destroy,c,load_object_id
   ```

   Notes:
   - Destroying the load object cleans the load object record objects that are generated by the loading process and old state information.
   - If you created the dump file by using a script, move the dump file to archival storage or destroy it after you successfully load the file. You cannot successfully execute the script again
if you leave the dump file in the location where the script created it. Content Server does not overwrite an existing dump file with another dump file of the same name.

- If Content Server crashes during a load, you can fetch the Load Object and save it again, to restart the process. Content Server begins where it left off when the crash occurred.

**DocApps**

DocApps are not dumped when you dump a repository. Consequently, after you load a new repository, install and run the DocApp installer to reinstall the DocApps in the newly loaded repository.

**Generating dump and load trace messages**

You can activate tracing during dump and load operations to generate trace messages in the Content Server session log.

To activate tracing, use a `setServerTraceLevel` method.

The trace information includes:

- Whether Content Server fails to dump or load an object
- The query used to search for matching objects for a dump or load operation
- The current progress and status of a dump or load operation

**Repository maintenance**

Repositories should be cleaned up regularly as part of a maintenance schedule. Cleaning a repository involves removal of:

- Orphaned content files
  When users delete a document, or any object that has a content file associated with it, the system deletes the object and marks the content as an orphan. The system does not delete the actual content file. This must be done using the `dmclean` utility.
- Unwanted document versions and renditions
- Orphaned annotations and internal ACLs
  An annotation is orphaned when it is detached from all documents or other objects to which it was attached.
  An internal ACL is orphaned when it is no longer referenced by any object.
- Aborted workflows
  A workflow that has been stopped by the execution of an Abort method is an aborted workflow.
- Old log files
To clean a repository:

1. Perform a complete backup of the repository.

2. Delete unwanted versions of documents.
   You can delete only versions created before a certain date or by a certain author or delete all but the CURRENT version from one or more version trees.
   - To delete selected versions of documents, use the DELETE...OBJECT statement.
     Identify the documents to delete by their creation date, modification date, or some other criteria that you choose. For example, the following statement deletes all documents that have not been changed since January 1, 2000:
     ```
     DELETE "dm_document" OBJECTS
     WHERE "r_modify_date" < DATE('01/01/2000')
     ```
   - To delete versions from a version tree, use a IDISysObject.prune method.
     Prune deletes all unwanted versions on a specified tree or branch of a tree. An unwanted version is any version that has no symbolic label and that does not belong to a virtual document. Refer to the Javados for the usage of the method.

3. Delete unused renditions.
   A rendition is represented in the repository by a content object that points to the source document and by a content file.
   To delete a rendition (without deleting its source document, first update the content object for the rendition to remove its reference to the source document.
   For example, the following UPDATE...OBJECT statement updates all server- and user-generated renditions created before January 1, 2000. The updates in the statement detach the affected renditions from their source documents, effectively deleting them from the repository.
   ```
   UPDATE "dmr_content" OBJECTS
   SET "parent_count" = 0,
   TRUNCATE "parent_id",
   TRUNCATE "page"
   WHERE "rendition" != 0 AND "set_time" < DATE('01/01/2000')
   ```

4. Clean the temp directory by deleting the temporary files in that location.
   You can determine the location of the temp directory with the following query:
   ```
   SELECT "file_system_path" FROM "dm_location"
   WHERE "object_name" = 'temp'
   ```

5. Delete any unwanted dmi_queue_item objects.
   Every time an object is placed in the inbox of a user, a dmi_queue_item object is created. When the object is removed, the queue item object is not destroyed, but it is marked in the repository as dequeued. Use the DELETE...OBJECT statement to remove dmi_queue_item objects.
   For example, the following statement removes all queue items objects that were dequeued before January 1, 2000:
   ```
   DELETE "dmi_queue_item" OBJECTS
   WHERE "dequeued_date" < DATE('01/01/2000')
   AND "delete_flag"=true
   ```

6. Run the dmclean utility to remove orphaned content files, orphaned annotations and ACLs, and aborted workflows. You can execute the Dmclean administration tool or run the dmclean utility manually. Dmclean (dm_DMClean), page 192 provides more information about the dmclean utility.
7. Delete or archive old server logs, session logs, trace files, and old versions of the product.
   Session logs are located in the %DOCUMENTUM%/dba/log/repository_id ($DOCUMENTUM/dba/log/repository_id) directory.

   Content Server and connection broker log files are found in the %DOCUMENTUM%/dba/log ($DOCUMENTUM/dba/log) directory. The server log for the current server session is named repository_name.log. The log for the current instance of the connection broker is named docbroker.docbroker_hostname.log. Older versions of these files have the extension .save and the time of their creation appended to their name.

   On Windows, you can use the del command or the File Manager to remove unwanted session logs, server logs, and connection broker logs. On Linux, use the rm command.

### Checking consistency

Content Server provides the Consistency Checker, a tool that scans a repository and reports any inconsistencies. Inconsistencies typically include type or object corruptions, objects that reference a user, group, or other object that does not exist, and so forth. The tool does not fix the inconsistencies. Contact Documentum Technical Support for assistance in correcting errors found by the consistency checker.

The Consistency Checker tool is a job that can be run from the command line or using Documentum Administrator. Running jobs, page 225 provides information about running the job in Documentum Administrator.

The job generates a report that lists the checked categories and any inconsistencies that were found. The report is saved in the /System/Sysadmin/Reports/ConsistencyChecker directory. If no errors are found, the current report overwrites the previous report. If an error is found, the current report is saved as a new version of the previous report. By default, the Consistency Checker job is active and runs once a day.

EMC Documentum recommends to run this tool on a repository before upgrading the repository to a new version of the Documentum Server.

### Running the job from a command line

The Consistency Checker job is implemented as the consistency_checker.ebs script. To run the script from the command line, enter the following syntax at the command-line prompt:

dmbasic -fconsistency_checker.ebs -eEntry_Point --repository_name superuser password

Where repository_name is the name of the repository that is checked, superuser is the user name of a repository superuser, and password is the password of the superuser account.

The results of the checks are directed to standard output.
Example report

The following example describes a Consistency Checker report. In this case, the tool detected five inconsistencies in the Users & Groups section.

Beginning Consistency Checks.....
Repository Name: buzzard
Server Version: 5.1.0.63 Win32.SQLServer
Database: SQLServer
#################################################
##
## CONSISTENCY_CHECK: Users & Groups
## Start Time: 09-10-2002 10:15:55
##
##
Checking for users with non-existent group
- WARNING CC-0001: User 'docu' belongs to non-existent group ''
- WARNING CC-0001: User 'engr' belongs to non-existent group ''
- WARNING CC-0001: User 'marketing' belongs to non-existent group ''
- WARNING CC-0001: User 'nagboat' belongs to non-existent group ''
- WARNING CC-0001: User 'admingroup' belongs to non-existent group ''
Rows Returned: 5
Checking for users belonging to groups not in dm_user
Checking for users not listed in dmi_object_type
Checking for groups not listed in dmi_object_type
Checking for groups belonging to non-existent groups
Checking for groups with non-existent super groups
#################################################
##
##
## CONSISTENCY_CHECK: ACLs ##
## Start Time: 09-10-2002 10:15:55
##
##
Checking for ACLs with non-existent users
Checking for ACLs with missing dm_acl_r table entries
Checking for sysobjects with acl_domain set to non-existent user
Checking for sysobjects that belong to non-existent users
Checking for sysobjects with non-existent ACLs
Checking for ACL objects with missing dm_acl_s entry
Checking for ACL objects with r_accessor_permit value but missing r_accessor_name value
Checking for ACL objects with r_accessor_name value
Checking for ACL objects with r_is_group value but missing r_accessor_permit value
Checking for ACL objects with r_is_group value but missing r_accessor_name value
Checking for ACL object with r_accessor_name value
but missing r_is_group value
Checking for ACL object with r_accessor_permit value
but missing r_is_group value

Checking for sysobjects which are not referenced in dmi_object_type
Checking for sysobjects that point to non-existent content
Checking for sysobjects that are linked to non-existent folders
Checking for sysobjects that are linked to non-existent primary cabinets
Checking for sysobjects with non-existent i_chronicle_id
Checking for sysobjects with non-existent i_antecedent_id
Checking for sysobjects with missing dm_sysobject_r entries
Checking for sysobjects with missing dm__sysobject_s entry

Checking for folders with missing dm_folder_r_table entries
Checking for folders that are referenced in dm_folder_r
but not in dm_folder_s
Checking for dm_folder objects that are missing an entry in dmi_object_type
Checking for dm_folder objects that are missing corresponding dm_sysobject entries
Checking for folders with non-existent ancestor_id
Checking for cabinet that have missing dm_folder_r_table entries
Checking for cabinets that are missing an entry in dmi_object_type
Checking for folder objects with missing dm_sysobject_r entries
Checking for folder objects with null r_folder_path

Checking for documents with missing dm_sysobject_r entries
Checking for documents with null r_folder_path

EMC Documentum Administrator Version 7.2 User Guide
Checking for documents with a dm_sysobject_s entry but no dm_document_s entry
Checking for documents with missing dm_sysobect_s entries
Checking for documents with missing dmi_object_type entry

#################################################
##
## CONSISTENCY_CHECK: Content
##
## Start Time: 09-10-2002 10:16:03
##
##
##
checking for content objects that reference non-existent parents
Checking for content with invalid storage_id
Checking for content objects with non-existent format

#################################################
##
## CONSISTENCY_CHECK: Workflow
##
## Start Time: 09-10-2002 10:16:03
##
##
##
Checking for dmi_queue_item objects with non-existent queued objects
Checking for dmi_workitem objects that reference non-existent dm_workflow objects
Checking for dmi_package objects with missing dmi_package_s entries
Checking for dmi_package objects that reference non-existent dm_workflow objects
Checking for workflow objects with non-existent r_component_id
Checking for workflow objects with missing dm_workflow_s entry
Checking for work item objects with missing dm_workitem_s entry

#################################################
##
## CONSISTENCY_CHECK: Types
##
## Start Time: 09-10-2002 10:16:04
##
##
##
Checking for dm_type objects with a non-existent dmi_type_info object
Checking for dmi_type_info objects with a non-existent dm_type object
Checking for type objects with corrupted property positions
Checking for types with invalid property counts
Basic Configuration

#################################################
##
## CONSISTENCY CHECK: Data Dictionary
##
## Start Time: 09-10-2002 10:16:04
##
##
Checking for duplicate dmi_dd_attr_info objects
Checking for duplicate dmi_dd_type_info objects
Checking for any dmi_dd_attr_info objects that are missing an entry in dmi_dd_common_info_s
Checking for any dmi_dd_type_info objects that are missing an entry in dmi_dd_common_info_s
Checking for any dmi_dd_attr_info objects that are missing an entry in dmi_dd_attr_info_s
Checking for any dmi_dd_type_info objects that are missing an entry in dmi_dd_type_info_s

#################################################
##
## CONSISTENCY CHECK: Lifecycles
##
## Start Time: 09-10-2002 10:16:11
##
##
Checking for sysobjects that reference non-existent policy objects
Checking for any policy objects that reference non-existent types in included_type
Checking for any policy objects with missing dm_sysobject_s entry
Checking for any policy objects with missing dm_sysobject_r entries
Checking for policy objects with missing dm_policy_r entries
Checking for policy objects with missing dm_policy_s entry

#################################################
##
## CONSISTENCY CHECK: FullText
##
## Start Time: 09-10-2002 10:16:11
##
##
Checking for tdk index objects that point to non-existent fulltext index objects
Checking for any tdk collect objects that point to non-existent tdk index objects
Checking for any fulltext index objects that point to non-existent tdk index objects
Checking for any tdk index objects that point to non-existent tdk collect objects
Checking for any non-orphaned dmr_content objects that point to types that do not exist
Checking for any non-orphaned dmr_content objects that point to non-existent formats
Checking for any dmr_content objects that point to a non-existent fulltext index
Checking for any fulltext index properties that are...
no longer in dm_type

Checking for dmi_index objects that reference non-existent types
Checking for types with non-existent dmi_index object for <type>_s table
Checking for types with non-existent dmi_index object for <type>_r table
Checking for index objects with invalid property positions

Checking for java dm_method objects that reference jview

Consistency Checker completed successfully
Total number of inconsistencies found: 5
Disconnected from the server.

## Changing the repository owner password

If you need to change the password in the database used by the repository owner account (also referred to as the database owner account, and listed as database_owner in the server.ini file), use the following procedure:

1. Shutdown the repository.
2. Change the repository owner account password in the database.
3. Edit the dbpasswd.txt file to contain one line with the new password in plain text.
4. Encrypt the dbpasswd.txt file. From the $DM_HOME/bin directory, use the command:
   ```bash
dm_encrypt_password -docbase <docbase_name> -rdbms -encrypt <database_password>
   ```
5. Start the repository.
Windows domain authentication for Linux repositories

A repository on a Linux host can use Windows domain authentication to authenticate repository users. Configuring Windows domain authentication for Linux repositories requires the following:

- Defining a domain map that includes the Windows domain, as described in Creating or modifying a domain map, page 65 and Defining a domain, page 66.
- Configure repository users for Windows domain authentication, as described in Modifying users for Windows domain authentication, page 66.
- Modifying the dm_check_password program to work with Windows domain authentication.
- Modifying the user_source property in the user object for each user in the Linux repository.

Each user in a Linux repository must have the user_source property set to domain only, Unix first, or domain first. You can modify the property with Documentum Administrator on the User page.

**Note:** Linux 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 Linux 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 Map 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 Linux repository. Defining a domain, requires the primary controller name of the domain and any backup controllers' names. 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.
   The domain name is a required field.
2. Type the primary controller name.
   The primary controller name is a required field.
3. Type the backup controller domain name.
   The backup controller domain name 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 Linux 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 Linux authentication.
4. Click OK to save the changes and return to the Users list page.
Managing Content Servers

The default Content Server installation creates a repository with one server. In Documentum Administrator, administrators can configure additional servers to run against a particular repository.

Each Content Server is associated with a server configuration object. A server configuration object is a template for a Content Server. A server configuration is defined by the properties in the associated server configuration object and the parameters in the server.ini file that is read during server startup. At startup, a server always reads the CURRENT version of its server configuration object.

All server configuration objects for the current repository are listed on the Content Server Configuration page in Documentum Administrator, as described in Table 7, page 67.

Server configuration objects are stored in the repository System cabinet. You can add Content Servers by creating 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:** The *EMC Documentum Content Server Installation Guide* and *EMC Documentum Content Server Distributed Configuration Guide* provides information about creating, starting, and stopping a remote Content Server.

**Table 7. Server configuration object information**

<table>
<thead>
<tr>
<th>Column</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>The name of the server configuration object.</td>
</tr>
<tr>
<td>Host</td>
<td>The name of the host on which the Content Server associated with the server configuration object is running.</td>
</tr>
<tr>
<td>Operational Status</td>
<td>The current running status and dormancy status separated by a comma of the Content Server. Valid values:</td>
</tr>
<tr>
<td></td>
<td>Running Status:</td>
</tr>
<tr>
<td></td>
<td>• Running</td>
</tr>
<tr>
<td></td>
<td>• Unknown</td>
</tr>
<tr>
<td></td>
<td>Dormancy Status:</td>
</tr>
<tr>
<td></td>
<td>• Dormancy Requested</td>
</tr>
<tr>
<td></td>
<td>• Dormant</td>
</tr>
<tr>
<td></td>
<td>• Active</td>
</tr>
<tr>
<td></td>
<td>• Invalid</td>
</tr>
<tr>
<td></td>
<td><strong>Note:</strong> The Operational Status column will display only the current running status for Content Server versions prior to 7.0.</td>
</tr>
<tr>
<td>Version</td>
<td>The version of the server configuration object.</td>
</tr>
</tbody>
</table>
Adding or modifying Content Servers

The Server Configuration list page in Documentum Administrator lists the server configuration objects of all Content Servers for the current repository. Each Content Server has a server configuration object in the repository.

To create, view, or modify server configuration object properties:

1. Log in to Documentum Administrator.
2. Select Administration > Basic Configuration > Content Servers.
   The Content Server Configuration page displays.
3. On the Content Server Configuration page, do one of the following:
   • To add a Content Server, select File > New > Server Config.
   • To modify the server configuration object of an existing Content Server, select the server configuration object in the Name column, then select View > Properties > Info.

   The Server Configuration Properties page displays.

   The Server Configuration Properties page is organized into tabbed pages as follows:

   Table 8. Server Configuration properties tabs

<table>
<thead>
<tr>
<th>Tab</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Info</td>
<td>Select the <strong>Info</strong> tab to view or modify information on the server host, the platform on which the server is running, code pages and locales, and other general information. <strong>Modifying general server configuration information, page 70</strong> provides the instructions.</td>
</tr>
<tr>
<td>Tab</td>
<td>Description</td>
</tr>
<tr>
<td>------------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Connection Brokers</td>
<td>Select the <strong>Connection Brokers</strong> tab to view or modify connection broker projections, as described in Creating or modifying connection broker projections, page 75.</td>
</tr>
<tr>
<td>Network Locations</td>
<td>Select the <strong>Network Locations</strong> tab to view or modify the proximity values for the associated network locations, as described in Creating or modifying network locations, page 76.</td>
</tr>
<tr>
<td>App Servers</td>
<td>Select the <strong>App Servers</strong> tab to add an application server for Java method execution, as described in Creating or modifying application servers, page 77.</td>
</tr>
<tr>
<td>Cached Types</td>
<td>Select the <strong>Cached Types</strong> tab to specify which user-defined types are to be cached at server startup, as described in Creating or modifying cached types, page 78.</td>
</tr>
<tr>
<td>Locations</td>
<td>Select the <strong>Locations</strong> tab to view the locations of certain files, objects, and programs that exist on the server host file system, including the assume user program, change password program, log file. Creating or modifying locations, page 78 provides instructions on creating or modifying locations.</td>
</tr>
<tr>
<td>Far Stores</td>
<td>Select the <strong>Far Stores</strong> tab to view accessible storage areas and to designate far stores, as described in Creating or modifying far stores, page 79. A server cannot store content in a far store. The <em>EMC Documentum Distributed Configuration Guide</em> provides more information about far stores.</td>
</tr>
</tbody>
</table>

If you are creating a server configuration object, start with the Info page and proceed sequentially through the tabs. However, the easiest way to create a server configuration object is to copy an existing server configuration object and then modify the new server configuration object properties, as described in Duplicating a server configuration object, page 69.

**Duplicating a server configuration object**

Use these instructions to create a server configuration object using an existing server configuration object as a template. Create a server configuration object when you run additional servers against a repository, whether on the same host or a different host.

**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. In the Name field, type the name of the new server configuration object.
5. Modify any properties that you want to change. Adding or modifying Content Servers, page 68 provides information on modifying the other properties.
6. Click OK to save the new server configuration object or Cancel to exit.
Note: This option will be disabled if the Content Server is in dormant state for 7.0 and later versions of Content Server.

Modifying general server configuration information

Use these instructions to create or modify the general server information, such as the server host, the platform on which the server is running, code pages and locales.

To modify general server configuration information:

1. Navigate to Administration > Basic Configuration > Content Servers.
   The Content Server Configuration list page displays.
2. On the Content Server Configuration page, do one of the following:
   - To create a new server configuration object, select File > New > Server Config.
   - To modify an existing server configuration object, select the server configuration object in the Name column, then select View > Properties > Info.
   The Server Configuration Properties page displays with the Info tab selected.
3. Enter or modify the server configuration object properties, as described in the following table:

   Table 9. General server configuration properties

<table>
<thead>
<tr>
<th>Field label</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>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.</td>
</tr>
<tr>
<td>Host Name</td>
<td>The name of the host on which the server is installed. Read-only.</td>
</tr>
<tr>
<td>Server Version</td>
<td>The version, operating system, and database of the server defined by the server configuration object. Read-only.</td>
</tr>
<tr>
<td>Process ID</td>
<td>The server’s process ID on its host. Read-only.</td>
</tr>
<tr>
<td>Install Owner</td>
<td>The Documentum installation owner. Read-only.</td>
</tr>
<tr>
<td>Install Domain</td>
<td>On Windows, the domain in which the server is installed and running. Read-only.</td>
</tr>
<tr>
<td>Trusted Mode</td>
<td>Indicates whether Trusted Content Services is enabled. Read-only.</td>
</tr>
<tr>
<td>Dormancy Status</td>
<td>Indicates the dormancy status of Content Server.</td>
</tr>
</tbody>
</table>

   Note: The Dormancy Status label is only visible for 7.0 and later versions of Content Server.

Update Configuration Changes
### Basic Configuration

<table>
<thead>
<tr>
<th>Field label</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Re-Initialize Server</td>
<td>Select to reinitialize the server after the server configuration object is saved.</td>
</tr>
</tbody>
</table>

#### Configuration Changes

- **Web Server Location**
  The name of the web server host and its domain. Used by client applications for creating DRLs.

- **Web Server Port**
  Identifies the port the web server uses. The default is 80.

- **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.

- **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.
<table>
<thead>
<tr>
<th>Field label</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Keep Entry Interval</td>
<td>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).</td>
</tr>
<tr>
<td>Locale Name</td>
<td>Indicates the server locale. The value is determined during server installation.</td>
</tr>
<tr>
<td>Default Client Codepage</td>
<td>The default codepage for clients. The value is determined programmatically and is set during server installation. In general, it does not need to be changed.</td>
</tr>
<tr>
<td></td>
<td>Options are:</td>
</tr>
<tr>
<td></td>
<td>• UTF-8</td>
</tr>
<tr>
<td></td>
<td>• ISO_8859-1</td>
</tr>
<tr>
<td></td>
<td>• Shift_JIS</td>
</tr>
<tr>
<td></td>
<td>• EUC-JP</td>
</tr>
<tr>
<td></td>
<td>• EUC-KR</td>
</tr>
<tr>
<td></td>
<td>• US-ASCII</td>
</tr>
<tr>
<td></td>
<td>• ISO_10646-UCS-2</td>
</tr>
<tr>
<td></td>
<td>• IBM850</td>
</tr>
<tr>
<td>Server OS Codepage</td>
<td>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, this value is not changed.</td>
</tr>
<tr>
<td></td>
<td>Options are:</td>
</tr>
<tr>
<td></td>
<td>• UTF-8</td>
</tr>
<tr>
<td></td>
<td>• ISO_8859-1</td>
</tr>
<tr>
<td></td>
<td>• Shift_JIS</td>
</tr>
<tr>
<td></td>
<td>• EUC-JP</td>
</tr>
<tr>
<td></td>
<td>• EUC-KR</td>
</tr>
<tr>
<td></td>
<td>• US-ASCII</td>
</tr>
<tr>
<td></td>
<td>• ISO_10646-UCS-2</td>
</tr>
<tr>
<td>Field label</td>
<td>Value</td>
</tr>
<tr>
<td>--------------------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Turbo Backing Store</td>
<td>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.</td>
</tr>
<tr>
<td>Rendition Backing Store</td>
<td>The name of the file store storage area where the server will store renditions generated by full-text indexing operations.</td>
</tr>
<tr>
<td>Modifications Comments</td>
<td>Remarks on changes made to the server configuration object in this version.</td>
</tr>
<tr>
<td>SMTP Server</td>
<td>The name of the computer hosting the SMTP Server that provides mail services to Content Server.</td>
</tr>
<tr>
<td></td>
<td>The value is provided during server installation.</td>
</tr>
<tr>
<td>Workflow Agent Worker Threads</td>
<td>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.</td>
</tr>
<tr>
<td></td>
<td>Configuring the workflow agent, page 511 provides more information about workflows.</td>
</tr>
<tr>
<td>Secure Connect Mode</td>
<td>Specifies whether type of connection the server accepts. Options are:</td>
</tr>
<tr>
<td></td>
<td>• Dual: Uses encrypted and unencrypted connections.</td>
</tr>
<tr>
<td></td>
<td>• Native: Uses unencrypted connections only.</td>
</tr>
<tr>
<td></td>
<td>• Secure: Uses encrypted connections only.</td>
</tr>
<tr>
<td></td>
<td>If you change the mode, you must restart the server. Re-initializing the server does not suffice.</td>
</tr>
<tr>
<td>Maximum Content Migration</td>
<td>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.</td>
</tr>
<tr>
<td>Threads</td>
<td>This option requires a Content Storage Services license that is enabled on the Content Server.</td>
</tr>
</tbody>
</table>
### Field label | Value
---|---
System Shutdown Timeout | The time in seconds that the workflow agent attempts to shut down work items gracefully after receiving a shutdown command. The default value is 120 seconds.  
When the timeout value expires, the server takes over and shuts down the workflow agent. This feature is only applicable for repositories that use multiple Content Servers.  
If the timeout period is exceeded (or is set to zero), Content Server takes over and shuts down the workflow agent immediately.  
If the timeout period is a negative value, Content Server waits for the workflow agent threads to complete the automatic tasks held by workflow agent workers before shutting down gracefully.  
*Changing the system shutdown timeout, page 511 provides more information about system shutdown behavior.*

### Authorization Settings

Inherit Permission Set From | 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:  
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.  
A Type permission set is associated with the type definition for a SysObject or SysObject subtype. A Type permission set can only be used as a default permission set.  
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.

Default Alias Set | The default alias set for new objects. Click the Select Alias Set link to access the Choose an alias set page.
Creating or modifying connection broker projections

The connection broker is the intermediary between a client and the server when the client wants a repository connection. If a server is not known to at least one connection broker, no clients can connect to the repository associated with the server. 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.

When a client requests a connection to a repository, the connection broker sends the client the connection information for each server associated with the repository. The client can then choose which server to use.

You access the Connection Brokers page by selecting the Connection Brokers tab on the Server Configuration Properties page, as described in Adding or modifying Content Servers, page 68.
To create, modify, or delete connection broker projection targets:

1. On the Connection Broker page, you can:
   - Click Add to add a connection broker projection target.
   - Modify an existing projection target by selecting the target in the Target Host column, then click Edit.
   - Delete an existing connection broker by selecting a connection broker, then click Remove.

   The Connection Broker Projection for ACS Server page displays.

2. Enter or modify the projection target information, as described in Table 10, page 76.

3. Do one of the following:
   - If you are creating a server configuration object, click Next to configure network locations.
   - If you are modifying an existing server configuration object, click OK to save your changes or click another tab to make additional changes. To enable the changes, reinitialize the server. Restarting the server is not required.

Table 10. Projection target information

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Target Host</td>
<td>Type the name of the host on which the connection broker resides.</td>
</tr>
<tr>
<td>Port</td>
<td>Type the port number on which the connection broker is listening.</td>
</tr>
<tr>
<td>Proximity</td>
<td>Type the correct proximity value for the connection broker.</td>
</tr>
<tr>
<td>Note</td>
<td>Type a note about the connection broker.</td>
</tr>
<tr>
<td>Status</td>
<td>Select Enabled to enable projection to the connection broker.</td>
</tr>
</tbody>
</table>

Creating or modifying network locations

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

You access the Network Location page by selecting the Network Locations tab on the Server Configuration Properties page, as described in Adding or modifying Content Servers, page 68.

To create, modify, or delete network locations:

1. On the Network Locations page, you can:
   - Click Add to create a network location.
   - Delete an existing network location by selecting a network location in the Network location ID column, then click Remove.

2. To add network locations on the Choose Network Locations page, select a network location in the left column and click .

   The network locations move to the right-hand column.
3. Click **OK** to save the change or **Cancel** to exit without saving.

4. To change the proximity values for a network location, edit the **Proximity** field. Servers send a proximity value to each connection broker projection target. The proximity value represents the physical server proximity to the connection broker.

5. Select or clear the **Enabled** option to enable or disable the server projection to a network location.

6. Do one of the following:
   - If you are creating a new server configuration object, click **Next** to configure application servers.
   - If you are modifying an existing server configuration object, click **OK** to save your changes or click another tab to make additional changes. To enable the changes, reinitialize the server. Restarting the server is not required.

## Creating or modifying application servers

Content Server supports application servers in the server configuration object. The Content Server configuration object specifies the name and the URI of the associated application servers.

Content Server supports a wide variety of network-accessible application, personalization, portal, and e-commerce servers from enterprise vendors such as BEA, IBM, Microsoft, Oracle, Sun, and SAP. For more information about how to deploy an application server, refer to the vendor documentation that came with the application server.

You access the App Servers page by selecting the **App Servers** tab on the Server Configuration Properties page, as described in Adding or modifying Content Servers, page 68.

### To create, modify, or delete application servers:

1. On the App Servers page, you can:
   - Click **Add** to add an application server.
   - Modify an existing application server by selecting the application server in the Name column, then click **Edit**.
   - Delete an existing application server by selecting the application server in the Name column, then click **Remove**.

2. Add or modify information on the Application Server page, as described in Table 11, page 78.

3. Do one of the following:
   - If you are creating a new server configuration object, click **Next** to configure cached types.
   - If you are modifying an existing server configuration object, click **OK** to save your changes or click another tab to make additional changes. To enable the changes, reinitialize the server. Restarting the server is not required.
Basic Configuration

Table 11. Application server properties

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Type the application server name.</td>
</tr>
<tr>
<td>URI</td>
<td>Type the URI to the application server, in the following format:</td>
</tr>
<tr>
<td></td>
<td>http://host_name:port_number/servlet_path</td>
</tr>
</tbody>
</table>

Creating or modifying cached types

Cached types specify which user-defined types are to be cached at server startup. By default, no user-defined objects are cached.

You access the Cached Types by selecting the **Cached Types** tab on the Server Configuration Properties page, as described in Adding or modifying Content Servers, page 68.

**To create, modify, or delete cached types:**

1. On the Cached Types page, you can:
   - Click **Add** to add one or more cached types. The **Choose a type** page appears.
   - Delete an existing cached type by selecting the cached type, then click **Remove**.
2. To add one or more cached types on the **Choose a type** page, select one or more cached types in the left column and click ➤. The cache types move to the right-hand column.
3. Click **OK** to save your changes.
4. Do one of the following:
   - If you are creating a new server configuration object, click **Next** to configure locations.
   - If you are modifying an existing server configuration object, click **OK** to save your changes or click another tab to make additional changes. To enable the changes, reinitialize the server. Restarting the server is not required.

Creating or modifying locations

The Location tab lets you view and modify the locations of files, objects, and programs on the server hosts file system, including the assume user program, change password program, and log file.

You access the Locations page by selecting the **Locations** tab on the Server Configuration Properties page, as described in Adding or modifying Content Servers, page 68.

**To view or modify locations:**

1. On the Locations page, you can click **Select Location** next to the file, object, or program, to change the location, as described in Table 12, page 79.
   - The **Choose a location** page appears.
2. Select a **Location** and **File System Path**, then click **OK**.

3. Do one of the following:
   
   - If you are creating a new server configuration object, click **Next** to configure far stores.
   - If you are modifying an existing server configuration object, click **OK** to save your changes or click another tab to make additional changes. To enable the changes, reinitialize the server. Restarting the server is not required.

**Table 12. Locations page properties**

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

**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. The *EMC Documentum Distributed Configuration Guide* provides more information on distributed content environments.
You access the Far Store page by selecting the **Locations** tab on the Server Configuration Properties page, as described in **Adding or modifying Content Servers, page 68**.

**To add or remove a far store:**

1. On the Far Stores page, you can:
   - Click **Add** to add one or more far stores. The **Choose a storage** page appears.
   - Delete an existing far stores by selecting the far store, then click **Remove**.
2. To add one or more far stores on the **Choose a storage** page, select one or more far stores in the left column and click 
   ![image]
   The far stores move to the right-hand column.
3. Click **OK** to save your changes.
4. Click **OK** to save the changes. To enable the changes, reinitialize the server. Restarting the server is not required.

**Moving a server to dormant and active states**

This section describes how to move a server to a dormant state and back to an active state.

A Content Server can be moved to a dormant state only from an active state. To perform this operation, you should be a member of the dm_datacenter_managers, a privileged group whose membership is maintained by superusers. This feature is only applicable for 7.0 and later versions of Content Server.

**To move a server to a dormant state:**

1. Navigate to **Administration > Basic Configuration > Content Servers**.
   The **Content Server Configuration** list page appears.
2. Select a server configuration that needs to be made dormant.
3. On the Content Server Configuration page, do one of the following:
   - Select a server configuration object in the Name column, then select **Tools > Make Dormant**.
   - Select a server configuration object in the Name column and then right-click. From the available menu options, select **Make Dormant**.
4. In the confirmation page, click **OK** to confirm with the request to move a server to a dormant state or **Cancel** to exit.

   When you click **OK**, the Content Server Configuration page displays.

   The system displays the message **Content Server moved to dormant state successfully**.
Note:

- You cannot copy a server configuration using **File > Save As** when the Content Server is in dormant state because the **Save As** option is disabled.

- The **Connection Brokers** tab in **Server Configuration properties** page does not list the secondary connection broker configured in server.ini when the Content Server is in dormant state.

- For a WDK application to login to a repository in a dormant state, dmc_wdk_presets_owner, dmc_wdk_preferences_owner, and dm_bof_registry users should be a member of dm_datacenter_managers.

A Content Server can be moved back to an active state only from a dormant state. To perform this operation, you should be a member of the dm_datacenter_managers, a privileged group whose membership is maintained by superusers. This feature is only applicable for 7.0 and later versions of Content Server.

**To move a server to an active state:**

1. Navigate to **Administration > Basic Configuration > Content Servers**.
   The **Content Server Configuration** list page appears.

2. Select a server configuration that needs to be made active.

3. On the Content Server Configuration page, do one of the following:
   - Select a server configuration object in the Name column, then select **Tools > Make Active**.
   - Select a server configuration object in the Name column and then right-click. From the available menu options, select **Make Active**.

4. In the confirmation page, click **OK** to confirm with the request to move a server back to an active state or **Cancel** to exit.

When you click **OK**, the Content Server Configuration page displays.

The system displays the message **Content Server moved to active state successfully**.

**Note:** You can also project the active or dormant state of Content Server to the connection broker. The **Projecting active or dormant state of Content Server to connection broker**, page 82 section contains the instructions.

---

**Enabling or disabling save operation for a Content Server in dormant state**

You can perform the enable or disable save operation for a Content Server if you are a member of the dm_datacenter_managers, a privileged group whose membership is maintained by superusers. When you enable save operation for a Content Server which is in dormant state, you can perform create and update operations. By default, save operation is disabled. This feature is only applicable for 7.0 and later versions of Content Server.

**Caution:** To perform any of the view, create, update, or delete operations for a Content Server which is in dormant state, you as a member of the dm_datacenter_managers group should
execute the action **Enable Save Operation**, else view, create, update, or delete operations will fail.

You can request to move a server to dormant state, as described in *Moving a server to dormant and active states, page 80.*

Use these instructions to perform the enable save operation:

**To perform enable save operation:**

1. Navigate to **Administration > Basic Configuration > Content Servers**.
2. Select the dormant server you want to enable save operation.
3. On the Content Server Configuration page, do one of the following:
   - Select the server configuration object in the Name column, then select **Tools > Enable Save Operation**.
   - Select the server configuration object in the Name column and then right-click. From the available menu options, select **Enable Save Operation**.

   The Content Server Configuration page displays.
   The system displays the message **Successfully enabled the save operation**.

Use these instructions to perform the disable save operation:

**To perform disable save operation:**

1. Navigate to **Administration > Basic Configuration > Content Servers**.
2. Select the dormant server you want to disable save operation.
3. On the Content Server Configuration page, do one of the following:
   - Select the server configuration object in the Name column, then select **Tools > Disable Save Operation**.
   - Select the server configuration object in the Name column and then right-click. From the available menu options, select **Disable Save Operation**.

   The Content Server Configuration page displays.
   The system displays the message **Successfully disabled the save operation**.

**Projecting active or dormant state of Content Server to connection broker**

The dormancy status of Content Server can be projected to Connection Broker. To perform this operation, you should be a member of the dm_datacenter_managers, a privileged group whose membership is maintained by superusers. This feature is only applicable for 7.0 and later versions of Content Server.

**Note:**

- The **Project Dormant Status to Connection Broker** and **Project Active Status to Connection Broker** menu options are available only for Content Servers which is in active state. These options will not be available for Content Servers which is in dormant state. Therefore, you always can
perform the Project Dormant Status to Connection Broker operation first followed by Project Active Status to Connection Broker operation.

- For a WDK application to login to a repository in a dormant state, dmc_wdk_presets_owner, dmc_wdk_preferences_owner, and dm_bof_registry users should be a member of dm_datacenter_managers.

You can view or modify connection broker projections, as described in Creating or modifying connection broker projections, page 75.

Use these instructions to project the dormancy status of Content Server to connection broker:

**To project dormant state to connection broker:**

1. Navigate to Administration > Basic Configuration > Content Servers.
2. Select the active server you want to project as dormant to the connection broker.
3. On the Content Server Configuration page, do one of the following:
   - Select the server configuration object in the Name column, then select Tools > Project Dormant Status to Connection Broker.
   - Select the server configuration object in the Name column and then right-click. From the available menu options, select Project Dormant Status to Connection Broker.

   The Content Server Configuration page displays.

   The system displays the message Successfully projected dormant status to Connection Broker.

**To project active state to connection broker:**

1. Navigate to Administration > Basic Configuration > Content Servers.
2. Select the active server you projected as dormant to project as active to connection broker.
3. On the Content Server Configuration page, do one of the following:
   - Select the server configuration object in the Name column, then select Tools > Project Active Status to Connection Broker.
   - Select the server configuration object in the Name column and then right-click. From the available menu options, select Project Active Status to Connection Broker.

   The Content Server Configuration page displays.

   The system displays the message Successfully projected active status to Connection Broker.

**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.

**Note:** If you are connected to a secondary server, you see only the server and connection broker logs for that server.
To view server or connection broker logs:
1. Navigate to Administration > Basic Configuration > Content Servers.
2. Select the server configuration object of the server whose log you want to view.
3. Do one of the following:
   - Select View > Server Log, select the log to view, then click View Log.
     The server log is displayed.
   - Select View > Connection broker Log, select the log to view, then click View Log.
     The connection broker log is displayed.

To delete server log files, run the Log Purge tool. Log purge (dm_LogPurge), page 196 provides more information about the tool.

Deleting a server configuration object

Do not delete the CURRENT version of the server configuration object of an active server. You can safely delete the CURRENT version of the server configuration object of a server that is shut down, or old configuration object versions of an active server. 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.
   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.

Confirming object deletion

When you delete certain objects from a repository, 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.
Configuring a server as a process engine

If the Business Process Manager (BPM) application is installed in a repository and you have a license for process engines, you can configure a server as a process engine.

**To configure a server as a process engine:**
1. Connect to the repository where you want to configure a server as a process engine.
2. Navigate to Administration > Basic Configuration > Content Servers.
3. Select a server.
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.

**Note:** Documentum Administrator does not provide an interface for disabling the process engine server. The server can only be disabled by deleting the server instance in the /System/Workflow/Process Engine folder. Disabling a process engine server, page 85 provides the more information.

Disabling a process engine server

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, 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

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 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 EMC Documentum Distributed Configuration Guide.

Creating or modifying federations

Use these instructions to create a federation. Before you create a federation, obtain the user name and password of a superuser account 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.

The EMC Documentum Distributed Configuration Guide provides more information on federations.

To create or modify a federation:

1. Navigate to Administration > Basic Configuration > Federation.
   The Federations list page appears.

2. Do one of the following:
   - Select File > New > Federation to create a federation.
     The New Federation Configuration page appears.
     Select the governing repository of the new federation from the repository list and click Next.
     If you do not see a particular repository on the page, that repository is already a member of a federation.
   - Select the federation to modify and then select View > Properties > Info.
3. 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 or page or the Federation Configuration Properties - Info page.

4. Enter information for the federation, as described in Table 13, page 87.

5. Ensure that all repositories project to the same connection brokers.

**Table 13. Federation properties**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Info tab</strong></td>
<td></td>
</tr>
<tr>
<td>Name</td>
<td>Type the name of the new federation.</td>
</tr>
<tr>
<td>Make All Governing</td>
<td>Select to make all users and groups in the governing repository global users and global groups.</td>
</tr>
<tr>
<td>Repository Users &amp; Groups Global</td>
<td></td>
</tr>
<tr>
<td>Active</td>
<td>This option is available if you are modifying an existing federation. To change the status of an existing federation, select or clear the Active checkbox.</td>
</tr>
<tr>
<td><strong>User Subtypes tab</strong></td>
<td></td>
</tr>
<tr>
<td>Add</td>
<td>Click Add to add user subtypes.</td>
</tr>
<tr>
<td></td>
<td>If there are user subtypes in the repository, a list of user subtypes is displayed on the Choose a user subtype page. Select the user subtypes to propagated to member repositories.</td>
</tr>
<tr>
<td><strong>Members tab</strong></td>
<td></td>
</tr>
<tr>
<td>Add</td>
<td>Click Add to add member repositories.</td>
</tr>
<tr>
<td></td>
<td>Select the repositories that you want to be member repositories and click Add.</td>
</tr>
<tr>
<td></td>
<td>Click Edit to edit a member repository. The Edit button will be available only after adding more than one repository.</td>
</tr>
<tr>
<td></td>
<td>To remove any member repositories from the Selected Items list, select them and then click Remove.</td>
</tr>
<tr>
<td>Name</td>
<td>The login name of a superuser account that is configured for the repository.</td>
</tr>
<tr>
<td>Password</td>
<td>The password of a superuser account this is configured for the repository.</td>
</tr>
<tr>
<td>Skip this member and continue authentication</td>
<td>Select this option if you want to skip entering the name and password at this time.</td>
</tr>
</tbody>
</table>
Adding, modifying, or deleting federation members

You can add or delete federation member repositories using the Members tab on the Federation Configuration Properties page.

To add, modify, or delete federation members:

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.
4. Type the name and password of a user who has superuser privileges for the federation.
   The Federation Configuration Properties - Info page appears.
5. Click the Members tab to access the Federation Configuration Properties - Members page.
6. Do one of the following:
   - To add a member repository, click Add to access the Choose Member Repositories page.
     Locate the repository that you want to add, select the checkbox next to the repository name, then click Add and OK. Type the name and password of a user who has superuser privileges in the new member repository and click OK.
   - To edit a member repository, click Edit. The Edit button will be available only after adding more than one repository.
   - To delete a member repository, select the checkbox next to any members that you want to remove and click Remove, then click OK.
7. Click Finish.

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.
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 necessary, 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.

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. Click OK.

**Java Method Servers**

EMC Documentum includes Java Method Server (JMS), a customized version of JBoss to execute Content Server Java methods. One Java Method Server is installed with each Content Server installation. You can use Documentum Administrator to modify existing Java Method Servers, but you cannot add new Java Method Servers from the Documentum Administrator interface. To add a Java Method Server, you have to run the Content Server Configuration Program. The *EMC Documentum Content Server Enterprise Edition Installation Guide* provides more information about installing multiple Content Servers, Java Method Servers, and the supported JMS failover configurations.

EMC Documentum provides a servlet called DO_METHOD to execute Documentum Server methods. The compiled servlet code is found in the mthdservert.jar file located on the same host as Content Server. The file contains the IDmMethod class. Java Method Server runs as an independent process. The process can be stopped or started without recycling the Content Server. On Windows platforms, the Java Method Server can be run as a Windows service or as a process.

The method server itself is a Java-based web application. Each time a method is invoked, the Content Server makes an HTTP request passing the name of the Java class which implements the method along with any specified arguments to a servlet which knows how to execute the specified method.

**Note:** The Java method server can also be used to execute Java methods that are not associated with a method object. Use an HTTP_POST administration method to send the request to the Java method server. The *EMC Documentum Content Server DQL Reference Manual* provides details about the administration method.

Documentum Administrator provides a Java Method Server configuration page for
- Viewing and updating Java Method Servers.
- Associating Content Servers with Java Method Servers.
- Viewing the Java Method Server status information in the Content Server memory cache.
- Resetting the Java Method Server information in the Content Server memory cache.

**Viewing Java method server information**

All available Java Method Servers (JMS) are displayed on the Java Method Server Configuration page. Users with superuser or system administrator privileges can access the Java Method Server Configuration page. To access the page, log into a repository and navigate to Administration > Basic Configuration > Java Method Servers.

Each JMS is represented by a JMS configuration object. The Java Method Server Configuration page displays information for all Java method server configuration objects in the repository, as described in Table 14, page 91.
### Table 14. Java method server information

<table>
<thead>
<tr>
<th>Column label</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>The name of the JMS configuration object.</td>
</tr>
<tr>
<td>Is Enabled</td>
<td>Specifies whether the Java method server is enabled or disabled.</td>
</tr>
<tr>
<td>Associated Content Servers</td>
<td>The Content Server with which the JMS configuration object is associated.</td>
</tr>
</tbody>
</table>

The **Tools** menu on the Java Method Server Configuration page also provides the option to view information about all active Java method servers. Select **Tools > Active Java Method Servers List** to display the Active Java Method Servers List page. Viewing active Java method servers, page 93 provides the more information.

### Modifying a Java Method Server configuration

Only users with superuser privileges can modify Java Method Server (JMS) configurations.

**To modify Java method server configuration:**

1. Log in to the repository for which you want to modify the JMS configuration.
2. Select **Administration > Basic Configuration > Java Method Servers**
   - Java Method Server Configuration page displays.
3. Select the JMS configuration you want to modify, then select **View > Properties > Info** or right-click the JMS configuration object and select **Properties**.
   - The Java Method Server Configuration Properties page displays.
4. View or modify the information for the JMS configuration, as described in **Table 15, page 91**.

### Table 15. JMS configuration information

<table>
<thead>
<tr>
<th>Field label</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>The name of the JMS configuration.</td>
</tr>
<tr>
<td>Enable</td>
<td>Enables or disables the JMS.</td>
</tr>
<tr>
<td></td>
<td>Select this option to enable the JMS configuration or deselect to disable the JMS.</td>
</tr>
</tbody>
</table>

**Associated Content Servers**
### Basic Configuration

<table>
<thead>
<tr>
<th>Field label</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Content Server</td>
<td>The list of Content Servers that is associated with the JMS configuration. A JMS configuration can be associated with one or more Content Servers. The <em>EMC Documentum Content Server Enterprise Edition Installation Guide</em> provides more information about installing multiple Content Servers, Java Method Servers, and the supported JMS failover configurations.</td>
</tr>
</tbody>
</table>
| Content Server location | Specifies whether the JMS is associated with a remote Content Server. Valid values are:  
  - *Java Method Server for primary Content Server*: The associated Content Server is local.  
  - *Java Method Server for secondary (or additional) Content Server*: The associated Content Server is remote (RCS). |
| Add                 | Click *Add* to add and associate a Content Server with the JMS configuration. The Servlet URL Editor page displays. Select the Content Server and intended purpose, as described in *Adding or modifying associated Content Servers*, page 92. |
| Edit                | Select the Content Server and click *Edit* to modify the Content Server associated with the JMS configuration. The Servlet URL Editor page displays. Modify the intended purpose, as described in *Adding or modifying associated Content Servers*, page 92. |
| Remove              | Select the Content Server and click *Remove* to remove the Content Server from the JMS configuration. |

### Java Method Server Servlet URLs

<table>
<thead>
<tr>
<th>Field label</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>The name of the Java servlet.</td>
</tr>
<tr>
<td>URL</td>
<td>The location of the Java servlet.</td>
</tr>
</tbody>
</table>

### Adding or modifying associated Content Servers

Use the Associated Content Servers page to add or modify Content Servers that are associated with a Java Method Server.

**To add or modify associated Content Servers:**

1. Log in to the repository for which you want to create the JMS configuration.
2. Select *Administration > Basic Configuration > Java Method Servers*
Java Method Server Configuration page displays.

3. Select the JMS configuration you want to modify, then select View > Properties > Info or right-click the JMS configuration object and select Properties.
   The Java Method Server Configuration Properties page displays.

4. Do one of the following:
   • Click Add to associate a Content Server with the JMS.
   • Select a Content Server and click Edit to modify the failover behavior for the JMS.
   The Associated Content Servers page displays.

5. Enter the Content Server and JMS failover information, as described in Table 16, page 93.

Table 16. Associated Content Servers information

<table>
<thead>
<tr>
<th>Column label</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Content Server</td>
<td>The name of the Content Server associated with the JMS.</td>
</tr>
<tr>
<td></td>
<td>To add a Content Server, select the Content Server from the drop-down list.</td>
</tr>
<tr>
<td></td>
<td>The drop-down list displays Content Server that were previously installed on</td>
</tr>
<tr>
<td></td>
<td>the host machine using the Content Server Configuration program. The EMC</td>
</tr>
<tr>
<td></td>
<td>Documentum Content Server Enterprise Edition Installation Guide provides</td>
</tr>
<tr>
<td></td>
<td>more information about installing multiple Content Servers, Java Method</td>
</tr>
<tr>
<td></td>
<td>Servers, and the supported JMS failover configurations.</td>
</tr>
<tr>
<td>Content Server location</td>
<td>Specifies whether the JMS is associated with a remote Content Server.</td>
</tr>
<tr>
<td></td>
<td>Valid values are:</td>
</tr>
<tr>
<td></td>
<td>• <strong>Java Method Server for primary Content Server</strong>: The associated</td>
</tr>
<tr>
<td></td>
<td>Content Server is local.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Java Method Server for secondary (or additional) Content Server</strong>: The</td>
</tr>
<tr>
<td></td>
<td>associated Content Server is remote.</td>
</tr>
</tbody>
</table>

Viewing active Java method servers

All active Java method servers are displayed on the Active Java Method Servers List.

To display all active Java method servers:

1. Log in to a repository and navigate to Administration > Basic Configuration > Java Method Servers.
2. Select Tools > Active Java Method Servers List.
   The Active Java Methods Servers List page displays with the information described in Table 17, page 94.
   To reset the information on the Active Java Methods Servers List page, click Refresh.
Table 17. Active Java method server information

<table>
<thead>
<tr>
<th>Field label</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Associated Content Server</td>
<td>The Content Server with which the JMS cache is associated.</td>
</tr>
<tr>
<td>Last Refreshed Time</td>
<td>The last time the Content Server JMS cache was reset.</td>
</tr>
<tr>
<td>Incremental Wait Time on Failure</td>
<td>The time Content Server waits before contacting the JMS, if the JMS fails to respond.</td>
</tr>
<tr>
<td></td>
<td>The wait time is doubled each time the JMS fails to respond until the maximum wait time is reached.</td>
</tr>
<tr>
<td>Maximum Wait Time on Failure</td>
<td>The maximum wait time Content Server keeps trying to contact the JMS, if the JMS fails to respond.</td>
</tr>
<tr>
<td>Java Method Server in Use</td>
<td>The name of the active Java method server that was used last time.</td>
</tr>
</tbody>
</table>

Java Method Servers associated with the Content Server

<table>
<thead>
<tr>
<th>Name</th>
<th>The name of the JMS configuration object.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Is Enabled</td>
<td>Specifies whether the Java method server is enabled or disabled.</td>
</tr>
<tr>
<td>Status</td>
<td>The current status of the JMS configuration object.</td>
</tr>
<tr>
<td>Content Server location</td>
<td>Specifies whether the JMS is associated with a remote Content Server. Valid values are:</td>
</tr>
<tr>
<td></td>
<td>• Java Method Server for primary Content Server: The associated Content Server is local.</td>
</tr>
<tr>
<td></td>
<td>• Java Method Server for secondary (or additional) Content Server: The associated Content Server is remote.</td>
</tr>
<tr>
<td>Last Failure Time</td>
<td>The last time the JMS failed to respond.</td>
</tr>
<tr>
<td>Next Retry Time</td>
<td>The next time the Content Server tries to contact the JMS, if the JMS fails to respond.</td>
</tr>
<tr>
<td>Failure Count</td>
<td>The number of times the JMS failed to respond.</td>
</tr>
</tbody>
</table>

LDAP servers

An Lightweight Directory Access Protocol (LDAP) directory server is a third-party product that maintains information about users and groups. Documentum Content Servers use LDAP directory servers for two purposes:

- Manage users and groups from a central location.
- Authenticate users.

It is not necessary for all users and groups in a repository to be managed through an LDAP directory server. A repository can have local users and groups in addition to the users and groups managed...
through a directory server. You can use more than one LDAP directory server for managing users and groups in a particular repository.

Using an LDAP server provides a single place for making additions and changes to users and groups. Content Server runs a synchronization job to automatically propagate the changes from the directory server to all the repositories using the directory server.

The LDAP support provided by Content Server allows mapping LDAP user and group attributes to user and group repository properties or a constant value. When the user or group is imported into the repository or updated from the directory server, the repository properties are set to the values of the LDAP properties or the constant. The mappings are defined when Content Server creates the LDAP configuration. The mappings can be modified later.

Using an LDAP directory server includes 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.
- The LDAP synchronization job must have at least read access to a unique identifier on the directory server, as follows:
  - nsuniqueid on SunDirectory processor
  - objectguid on Active Directory Server
  - ibm-entryuuid on IBM
  - guid on Novell
  - orclguid on Oracle

Apart from the unique identifiers, all the attributes that have been mapped in the LDAP configuration object should also have read access in the directory server.

The *EMC Documentum Content Server Release Notes* for your Content Server version, provides information about certified LDAP servers.

### Viewing LDAP server configurations

LDAP directory server configurations are managed under the **Administration > Basic Configuration > LDAP Servers** node. You can configure and map your existing LDAP configuration to a Content Server. Each LDAP server is associated with an LDAP configuration object. You must have superuser privileges to create, view, modify, or delete LDAP configuration objects.

Select **Administration > Basic Configuration > LDAP Servers** to view all 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*. Table 18, page 96 describes the properties that are displayed on the LDAP Server Configuration page.

From the LDAP Server Configuration page, you can:

- 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

Table 18. LDAP Server Configuration page properties

<table>
<thead>
<tr>
<th>Field label</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>The name of the LDAP configuration object.</td>
</tr>
<tr>
<td>Hostname</td>
<td>The name of the host on which the LDAP directory server is running.</td>
</tr>
<tr>
<td>Port</td>
<td>The port number where the LDAP directory server is listening for requests.</td>
</tr>
<tr>
<td>SSL Port</td>
<td>The SSL port for the LDAP directory server.</td>
</tr>
<tr>
<td>Directory Type</td>
<td>The directory type used by the LDAP directory server.</td>
</tr>
<tr>
<td>Import</td>
<td>Indicates if users and groups, groups and member users, or users only are imported.</td>
</tr>
<tr>
<td>Sync Type</td>
<td>Indicates if synchronization is full or incremental.</td>
</tr>
<tr>
<td>Failover</td>
<td>Indicates if failover settings have been established for the primary server.</td>
</tr>
<tr>
<td>Enabled</td>
<td>Indicates whether the LDAP server is active.</td>
</tr>
</tbody>
</table>

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 overwritten by information in directory server in case synchronization type is set to full synchronization on Sync and Authentication tab.

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
To add or modify an LDAP server configuration:

1. Navigate to Administration > Basic Configuration > LDAP Servers. The system displays the LDAP Server Configuration page.

2. Do one of the following:
   - To add an LDAP server configuration, select File > New > LDAP Server Configuration.
   - To modify an LDAP server configuration, select the LDAP server configuration, then select View > Properties > Info.

3. Enter or modify the information on Info tab of the LDAP Server Configuration page, as described in LDAP Server Configuration properties, page 97.

4. Click the Sync & Authentication tab and enter or modify the information on the LDAP Server Configuration - Synch & Authentication page, as described in LDAP Server Sync & Authentication properties, page 100.

5. Click the Mapping tab and enter or modify the mapping information on the LDAP Server Configuration - Mapping page, as described in LDAP Server mapping properties, page 101.

6. Click the Failover tab and enter or modify the information on the LDAP Server Configuration - Failover page, as described in LDAP Server failover properties, page 103.

7. Click Finish when you have completed configuring the new LDAP server. Content Server creates an ldap<objectID>.cnt password when you create the LDAP configuration object. If you have more than one Content Server associated with the repository, the password file must be copied to each Content Server in the environment or authentication fails.

LDAP Server Configuration properties

Table 19, page 97 describes the properties on the Info tab of the LDAP Server Configuration page. The properties apply to new and existing LDAP configuration objects.

Table 19. LDAP Server Configuration Properties properties

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>The name of the new LDAP configuration object. This field is read-only if you are viewing or modifying the LDAP configuration object.</td>
</tr>
<tr>
<td>Status</td>
<td>Select the Enable this LDAP Configuration checkbox to enable the LDAP configuration.</td>
</tr>
<tr>
<td>Field</td>
<td>Description</td>
</tr>
<tr>
<td>--------------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Directory Type</td>
<td>Refer to the Release Notes for your version of Documentum Content Server to see which LDAP server versions are supported.</td>
</tr>
<tr>
<td></td>
<td>Options are:</td>
</tr>
<tr>
<td></td>
<td>• Sun One/Netscape/iPlanet Directory Server (default)</td>
</tr>
<tr>
<td></td>
<td>• Microsoft Active Directory</td>
</tr>
<tr>
<td></td>
<td>• Microsoft ADAM</td>
</tr>
<tr>
<td></td>
<td>• Oracle Internet Directory Server</td>
</tr>
<tr>
<td></td>
<td>• IBM Directory Server</td>
</tr>
<tr>
<td></td>
<td>• Novell eDirectory</td>
</tr>
<tr>
<td>Hostname / IP Address</td>
<td>The name of the host on which the LDAP directory server is running. Starting from the 7.0 release, use only the hostname and not the IP address. However, you can use both the hostname and IP address in pre-7.0 releases.</td>
</tr>
<tr>
<td>Port</td>
<td>The port number where the LDAP directory server is listening for requests. The default is 389.</td>
</tr>
<tr>
<td>Binding Name</td>
<td>The binding distinguished name used to authenticate requests to the LDAP directory server by Content Server or the check password program.</td>
</tr>
<tr>
<td>Binding Password</td>
<td>The binding distinguished password used to authenticate requests to the LDAP directory server by Content Server or the check password program.</td>
</tr>
<tr>
<td></td>
<td>The Binding Password field only appears on the New LDAP Server Configuration - Info page.</td>
</tr>
<tr>
<td>Confirm Password</td>
<td>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 page.</td>
</tr>
<tr>
<td>Set</td>
<td>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.</td>
</tr>
<tr>
<td>Use SSL</td>
<td>Specifies whether SSL is used for authentication.</td>
</tr>
<tr>
<td>SSL Port</td>
<td>Specifies the SSL port. This option only displays when the Use SSL option is selected. Enter 636 for the SSL port value.</td>
</tr>
</tbody>
</table>
Follow these manual steps for SSL validation for 6.5x and below Content Servers:

1. Depending on the operating system (other than Windows 64-bit) on which the application server is installed, copy all the jar files from $Application_root$/WEB-INF/thirdparty/$osname$/ to $Application_root$/WEB-INF/lib

   For example, if the operating system on which the DA application is installed is Windows, copy all the jar files from $Application_root$/WEB-INF/thirdparty/win32/ to $Application_root$/WEB-INF/lib

   If the operating system on which the application server is installed is Windows 64-bit and the application server is using 64-bit JDK, do the following:
   1. Backup the jss311.jar file and delete it from $Application_root$/WEB-INF/lib
   2. Copy the jss42.jar file from $Application_root$/WEB-INF/thirdparty/win64/6.0.6 to $AppServer_root$/WEB-INF/lib

2. Depending on the operating system (other than Windows 64-bit) on which the application server is installed, copy all *.dll, (for Windows) or *.so (for Linux) files from $Application_root$/WEB-INF/thirdparty/$osname$/ to $AppServer_root$/da_dlls

   Note: If the da_dlls folder does not exist in the above specified location, create it.

   For example, if the operating system on which the DA application is installed is Windows, copy all the dll files from $Application_root$/WEB-INF/thirdparty/win32/ to $Application_root$/da_dlls

   If the operating system on which the application server is installed is Windows 64-bit and the application server is using 64-bit JDK, do the following:
   1. Copy the Microsoft.VC90.DebugCRT.manifest file from $Application_root$/WEB-INF/thirdparty/win64/6.0.6 to $AppServer_root$/da_dlls
   2. Copy all *.dll files from $Application_root$/WEB-INF/thirdparty/win64/6.0.6 to $AppServer_root$/da_dlls
3. Set the path of the dlls in startup batch file of the application server.
   • For Windows operating system: PATH=${AppServer_root}\da_dlls;%PATH%;
   • For Linux operating system: LD_LIBRARY_Path=${AppServer_root}/da_dlls;%LD_LIBRARY_PATH%:

**LDAP Server Sync & Authentication properties**

Table 20, page 100 describes the properties on the Sync & Authentication tab of the LDAP Server Configuration page. The properties apply to new and existing LDAP configuration objects.

**Table 20. LDAP Server Sync & Authentication properties**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Import</td>
<td>Specifies how users and groups are imported. Available options are:</td>
</tr>
<tr>
<td></td>
<td>• Users and groups (default)</td>
</tr>
<tr>
<td></td>
<td>• Users only</td>
</tr>
<tr>
<td></td>
<td>• Groups &amp; member users</td>
</tr>
<tr>
<td>Synchronize Nested Groups in the repository</td>
<td>Select to synchronize the nested groups in the repository.</td>
</tr>
<tr>
<td></td>
<td><strong>Note:</strong> This option is enabled only if Import field has the value Users and groups or Groups &amp; member users. This option is disabled if you select Users only for Import field.</td>
</tr>
<tr>
<td>Sync Type</td>
<td>Specifies how users and groups are synchronized. Available options are:</td>
</tr>
<tr>
<td></td>
<td>• Full: Import all based on user/group mappings (default)</td>
</tr>
<tr>
<td></td>
<td>• Incremental: Import only new or updated user/groups/members</td>
</tr>
<tr>
<td></td>
<td>If Groups and member users is selected in the Import field and a group was not updated but any of the group members were, the incremental synchronization is updating users identified by the user search filter.</td>
</tr>
<tr>
<td>Deleted Users</td>
<td>Specifies whether deleted user accounts are marked inactive. Available options are:</td>
</tr>
<tr>
<td></td>
<td>• set to inactive (default)</td>
</tr>
<tr>
<td></td>
<td>• unchanged</td>
</tr>
<tr>
<td>Update Names</td>
<td>Select to Update user names in repository or Update group names in repository.</td>
</tr>
<tr>
<td></td>
<td>The Update group names in repository checkbox is not enabled if Users Only is selected in the Import field.</td>
</tr>
</tbody>
</table>
**Basic Configuration**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>User Type</td>
<td>Select a user type. The default is dm_user.</td>
</tr>
<tr>
<td>Bind to User DN</td>
<td>Options are:</td>
</tr>
<tr>
<td></td>
<td>• Search for DN in directory using user’s login name</td>
</tr>
<tr>
<td></td>
<td>• Use DN stored with user record in repository (default)</td>
</tr>
<tr>
<td>External Password Check</td>
<td>Select to use external password check to authenticate users to directory.</td>
</tr>
</tbody>
</table>

The LDAP synchronization job must have at least read access to a unique identifier on the directory server, as follows:

- **nsuniqueid** on Sun One/Netscape/iPlanet Directory Server
- **objectguid** on Microsoft Active Directory Server
- **ibm-entryuuid** on IBM Directory Server
- **guid** on Novell eDirectory
- **orclguid** on Oracle Internet Directory Server

Apart from the unique identifiers, all the attributes that have been mapped in the LDAP configuration object should also have read access in the directory server.

**LDAP Server mapping properties**

Table 21, page 101 describes the properties on the Mapping tab of the LDAP Server Configuration page. The properties apply to new and existing LDAP configuration objects.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>User Object Class</td>
<td>Type the user object class to use for searching the users in the directory server.</td>
</tr>
</tbody>
</table>
| User Search Base    | Type the user search base. This is the point in the LDAP tree where searches for users start. For example:  
<p>|                     | cn=Users,ou=Server,dc=sds,dc=inengvm1llc,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 Search Filter field is populated with the resulting filter. |</p>
<table>
<thead>
<tr>
<th><strong>Field</strong></th>
<th><strong>Description</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>Group Object Class</td>
<td>Type the group object class to use for searching the groups in the directory server. Typical values are:</td>
</tr>
<tr>
<td></td>
<td>• For Netscape and Oracle LDAP servers: <code>groupOfUniqueNames</code></td>
</tr>
<tr>
<td></td>
<td>• For Microsoft Active Directory: <code>group</code></td>
</tr>
<tr>
<td>Group Search Base</td>
<td>Type the group search base. This is the point in the LDAP tree where searches for groups start. For example:</td>
</tr>
<tr>
<td></td>
<td><code>cn=Groups,ou=Server,dc=sds,dc=inengvm11c,dc=corp,dc=emc,dc=com</code></td>
</tr>
<tr>
<td>Group Search Filter</td>
<td>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 <code>cn=*</code></td>
</tr>
<tr>
<td>Search Builder</td>
<td>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</td>
</tr>
<tr>
<td></td>
<td>populated with the resulting filter.</td>
</tr>
<tr>
<td>Property Mapping</td>
<td>When a new configuration is added, this table populates with the mandatory mapping attributes. The mappings are dependent upon the directory type. This</td>
</tr>
<tr>
<td></td>
<td>table defines the pre-populated attributes and their mappings. All mapping types are LDAP Attribute.</td>
</tr>
<tr>
<td>Add</td>
<td>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</td>
</tr>
<tr>
<td></td>
<td>Documentum attribute maps or type in a custom value.</td>
</tr>
<tr>
<td>Edit</td>
<td>Select an attribute and then click Edit to access the Map Property page. On the Map Property page, edit the attribute properties.</td>
</tr>
<tr>
<td>Delete</td>
<td>Select an attribute and then click Delete to remove an attribute. The system displays the Deletion Confirmation page.</td>
</tr>
<tr>
<td>Repository Property</td>
<td>Displays the repository property that is the target of the mapping.</td>
</tr>
<tr>
<td>Type</td>
<td>Identifies the source of the property: User or Group.</td>
</tr>
<tr>
<td>Map To</td>
<td>Displays which attributes on LDAP that the property is mapped to.</td>
</tr>
<tr>
<td>Field</td>
<td>Description</td>
</tr>
<tr>
<td>-------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Map Type</td>
<td>Identifies the type of data: LDAP attribute, expressions, or a fixed constant.</td>
</tr>
<tr>
<td>Mandatory</td>
<td>Indicates if the mapping is mandatory for the attribute.</td>
</tr>
</tbody>
</table>

Content Server requires three properties to be defined for a user and one property to be defined for a group. The mandatory properties are:

- user_name
- user_login_name
- group_name

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.

### LDAP Server failover properties

Table 22, page 103 describes the properties on the Failover tab of the LDAP Server Configuration page. The properties apply to new and existing LDAP configuration objects.

Table 22. LDAP Server failover properties

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Failover Settings</td>
<td>Use this section to enter settings for the primary LDAP server.</td>
</tr>
<tr>
<td>Retry Count</td>
<td>The number of times Content Server tries to connect to the primary LDAP server before failing over to a designated secondary LDAP server. The default is 3. If the retry count value is set to 0, Content Server immediately reports that it failed to contact the primary LDAP directory server.</td>
</tr>
<tr>
<td>Retry Interval</td>
<td>Enter an interval number and select a duration (seconds, minutes, or hours) between retries. The default is at 3 seconds. Content Server fails to bind to the primary LDAP directory server, it waits the number of seconds specified before attempting to bind to the primary LDAP directory server again.</td>
</tr>
<tr>
<td>Field</td>
<td>Description</td>
</tr>
<tr>
<td>-------------------------</td>
<td>------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Reconnect</td>
<td>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.</td>
</tr>
<tr>
<td>Secondary LDAP Servers</td>
<td>Specifies secondary LDAP servers.</td>
</tr>
<tr>
<td></td>
<td>• To add a new secondary LDAP server, click Add. The Secondary LDAP Server page is displayed.</td>
</tr>
<tr>
<td></td>
<td>• To modify an existing secondary LDAP server, select the checkbox next to the name and click Edit. The Secondary LDAP Server page is displayed.</td>
</tr>
<tr>
<td></td>
<td>• To delete an existing secondary LDAP server, select the checkbox next to the name and click Delete.</td>
</tr>
<tr>
<td></td>
<td>• To reorder the list of LDAP servers, click Move Up or Move Down.</td>
</tr>
<tr>
<td>Name</td>
<td>Name of the secondary LDAP server.</td>
</tr>
<tr>
<td>Hostname</td>
<td>The name of the host on which the secondary LDAP directory server is running.</td>
</tr>
<tr>
<td>Port</td>
<td>The port information.</td>
</tr>
<tr>
<td>SSL Port</td>
<td>The SSL port number.</td>
</tr>
</tbody>
</table>

### Mapping LDAP Servers

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 configuration object. You can map the LDAP values to the following properties:

- System or user-defined properties
- Multiple directory values to a single repository property, using 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 given name 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.

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 can 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.

Table 23, page 105 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>
<thead>
<tr>
<th>DM attribute</th>
<th>DM type</th>
<th>LDAP attribute</th>
<th>Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>user_name</td>
<td>dm_user</td>
<td>cn</td>
<td>A</td>
</tr>
<tr>
<td>user_login_name</td>
<td>dm_user</td>
<td>uid</td>
<td>A</td>
</tr>
</tbody>
</table>

**Mapping guidelines**

The following rules apply when mapping LDAP group or user attributes to a repository property:

- In expressions, spaces are not required between references to LDAP attributes due to the bracket delimiter. If there is a space between mapped values, it appears in the result of the mapping.

- The length of the expression mapped to a single repository property cannot exceed 64 characters. Expressions that exceed 64 characters are truncated. The expression is recorded in the map_val property of the ldap config object. This property has a length of 64.

- All standard Documentum property lengths apply to the mappings. For example, the mapping string for user_name must resolve to 32 characters or less.

**Using Search Builder**

Access the Search Builder page by clicking the Search Builder button on the Mapping tab of the New LDAP Server Configuration or LDAP Server Configuration Properties 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**

On the Map Property page, you can add or modify mapping properties.
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**.

### Configuring secondary LDAP 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.

Enter the information for the secondary LDAP server, as described in Table 24, page 106.

#### Table 24. Secondary LDAP Server page properties

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Enter the name of the secondary LDAP server.</td>
</tr>
<tr>
<td>Hostname / IP Address</td>
<td>Type the name of the host on which the secondary LDAP directory server is running.</td>
</tr>
<tr>
<td>Port</td>
<td>The port information is copied from the primary LDAP server.</td>
</tr>
<tr>
<td>Binding Name</td>
<td>The binding name is copied from the primary LDAP server.</td>
</tr>
<tr>
<td>Binding Password</td>
<td>Type the binding distinguished password used to authenticate requests to the secondary LDAP directory server by Content Server or the check password program.</td>
</tr>
<tr>
<td>Confirm Password</td>
<td>Re-enter the binding password for verification.</td>
</tr>
<tr>
<td>Bind to User DN</td>
<td>The bind to user DN information is copied from the primary LDAP server.</td>
</tr>
<tr>
<td>Use SSL</td>
<td>The SSL information is copied from the primary LDAP server.</td>
</tr>
</tbody>
</table>
### 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 Info tab of the LDAP Server Configuration Properties 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 is 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 is 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 proxy server support**

Content Server supports LDAP proxy servers, for use in LDAP configurations. If you are using Global Catalog in Microsoft Active Directory Server, you have to ensure that all attributes required during LDAP synchronization are present in the Global Catalog.

**Configuring LDAP synchronization for Kerberros users**

LDAP synchronization in conjunction with Kerberos SSO authentication can be implemented in two different ways:

- Using an existing LDAP configuration to authenticate Kerberos users.
- Creating a new LDAP configuration to authenticate Kerberos users.

**To use an existing LDAP configuration to authenticate Kerberos users:**

1. Modify the user login domain attribute in the user object of all Kerberos users to use the short domain name instead of the name of the LDAP server.
   For example, if a Kerberos user is part of the wdkdomain.com domain, change the user login domain attribute to wdkdomain.
2. Change the user source attribute in the user object to dm_krb for all Kerberos users that are synchronized via LDAP, if the password is not in plug-in format. Changing the user source attribute is optional.
3. Run the LDAP synchronization job.

**To create a new LDAP configuration to authenticate Kerberos users**

1. Create an LDAP configuration object, as described in Adding or modifying LDAP server configurations, page 96. Use the short domain name as the LDAP configuration object name.
   For example, if Kerberos users are part of the wdkdomain.com domain, create an LDAP configuration object using wdkdomain as the LDAP configuration object name.
2. Change the user source attribute in the user object to dm_krb for all Kerberos users that are synchronized via LDAP.
3. Run the LDAP synchronization job.
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.

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

Viewing LDAP certificates

Content Server 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 certificate location that was specified when the LDAP server was added.

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: The version number of the certificate format.
   - 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 the certificate import fails.

Using multiple LDAP servers in SSL mode

Content Server supports running more than one LDAP server in SSL mode. Otherwise, LDAP synchronization does not work properly.

To set up multiple LDAP servers in SSL mode:

1. Identify a location for the certificate database.
The default location for the .cer certificate is ldapcertdb_loc. For .pem certificate browse and manually select the location object. The location object is created with the pem certificate name.

2. Import all required certificates into the certificate database, as described in Importing LDAP certificates, page 110.

3. Modify the certification location field for each LDAP server configuration that uses SSL to point to the same certificate database location.
   By default, Content Server assigns the file path that is specified in the ldapcertdb_loc object.

Replacing or removing LDAP certificates

Replacing, deleting or revoking of LDAP database certificates in the LDAP certificate database is not supported using the LDAP Certificate Management functionality. To update the certificates, manually remove the existing LDAP certificate database on the Content Server, restart the method server, then import the new certificates, as described in Importing LDAP certificates, page 110.
Chapter 3

Distributed Configurations

This chapter contains the following topics:

- Network locations, page 113
- ACS servers, page 117
- BOCS servers, page 123
- Configuring distributed transfer settings, page 128
- Messaging server configuration, page 130

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 could include network locations called San Francisco, New York, London, Athens, Tokyo, and Sydney, corresponding to users in those cities. A network location can 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.

Creating network locations requires superuser privileges. 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. Network locations should be created in the global registry repository that is defined when DFC is installed on the Documentum Administrator host. If a network contains multiple global registry repositories, a particular Documentum Administrator instance only recognizes the global registry that was designated during DFC installation on the Documentum Administrator host. You can connect to a global registry repository without being able to create network locations in that global registry.

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.
The *EMC Documentum Distributed Configuration Guide* provides more information about network locations.

**Creating, viewing, or modifying network locations**

Network locations should be created in the global registry repository that is defined when DFC is installed on the Documentum Administrator host. You must have superuser privileges in the global registry repository to create network locations. The *EMC Documentum Distributed Configuration Guide* provides 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. Therefore, when you create network locations, include the IP address 127.0.0.1 in a network location if you want to:

- Run a browser on the application server host where a WDK application is located.
- Use `localhost` in the URL when accessing the application.
- Automatically select the correct network location.

**To create, view, or modify network locations:**

1. Log in to the global repository that was created during DFC installation.
2. Select **Administration > Distributed Content Configuration > Network Locations**.
   
   The Network Locations page appears.
   
   If you do not see the Network Locations page, you are not connected to the correct global repository. Click **Global Registry Login** and connect to the correct repository.
3. Do one of the following:
   - Select **File > New > Network Location** to create a network location.
   - Select a network location, then **View > Properties > Info** to view or modify the network location properties.
4. Enter or modify the network location properties on the Info tab of the New Network Locations page or the Network Locations Properties page, as described in Table 25, page 114.
5. Click **OK** to save your changes.

**Table 25. Network location properties**

<table>
<thead>
<tr>
<th>Field label</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Network Location Identifier</td>
<td>An identifier that is used by system and network administrators. For example, to identify network locations by network subnets. This field cannot be edited after the network location is created.</td>
</tr>
<tr>
<td>Subject</td>
<td>A description of the network location.</td>
</tr>
</tbody>
</table>
### Distributed Configurations

<table>
<thead>
<tr>
<th>Field label</th>
<th>Value</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Default Network Location</td>
<td>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 location is used automatically and the user does not see the list.</td>
<td></td>
</tr>
<tr>
<td>Network Location Name</td>
<td>A descriptive name of the network location. For example, the geographical location of the network, such as Paris, San Francisco. The name is displayed on the login page for Documentum web clients when users must choose a network location. The display name is not the object name. The display name can be modified after the network location is created.</td>
<td></td>
</tr>
</tbody>
</table>
| IP Address Ranges                  | 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. Type the IP address 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 is 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:x:x:x:x:x:x or 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. |   |

## Copying network locations

To save time retyping existing information, 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 with superuser privileges to the global registry repository.
2. Select Administration > Distributed Content Configuration > Network Locations.
   The Network Locations page appears.

   **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 page appears. The fields display the values copied from the selected network location; however, the **Network Location Identifier** and **Network Location Name** fields display Copy [x] of [name]/[display name] to keep the network location and display names unique.

4. Modify the properties on Info tab of the Network Location Properties page.

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

### Deleting 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.

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 could not receive content in the most efficient manner possible.

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 do 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 **Network Location Name** and **Network Location Identifier** 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.

## ACS servers

An Accelerated Content Services (ACS) server is a light-weight server that is automatically created during a Content Server installation. The ACS server reads and writes content for web-based client applications using HTTP and HTTPS protocols. ACS servers do not modify object metadata but write content to storage areas.

Each Content Server host installation has one ACS server that communicates with one Content Server per repository and the Documentum Message Services (DMS) server. A single ACS server can serve content from multiple repositories. WDK-based applications can use the ACS server if the ACS server is enabled in the app.xml file of the applications.

Most ACS server properties can be modified using Documentum Administrator. Certain ACS server behavior is configured the acs.properties file on the ACS server host and cannot be modified by Documentum Administrator.

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

The ACS server is configured on the ACS Servers Configuration page that can be accessed in the **Administration > Distributed Content Configuration > ACS Servers** node. The ACS Servers Configuration page displays information about the ACS server, as described in Table 26, page 117.

### Table 26. ACS Server Configurations

<table>
<thead>
<tr>
<th>Column</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>The name that is assigned to the ACS server during the Content Server installation. The name cannot be modified.</td>
</tr>
<tr>
<td>Content Server</td>
<td>The name of the Content Server the ACS server is associated with.</td>
</tr>
<tr>
<td>Column</td>
<td>Description</td>
</tr>
<tr>
<td>-------------------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Content Access</td>
<td>Specifies how the ACS server can access content. Valid values are:</td>
</tr>
<tr>
<td></td>
<td>• <strong>Access all stores</strong>: The ACS server can access all stores that are connected to the Content Server.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Access local stores only</strong>: 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.</td>
</tr>
<tr>
<td></td>
<td>• <strong>None</strong> (disabled): The ACS server is disabled.</td>
</tr>
<tr>
<td>Projections &amp; Stores from</td>
<td>Specifies the connection broker projections, network locations, and local stores information for the ACS server.</td>
</tr>
<tr>
<td>Description</td>
<td>A description of the ACS server.</td>
</tr>
<tr>
<td>Dormancy Status</td>
<td>The current dormancy status of the ACS server. Valid values are:</td>
</tr>
<tr>
<td></td>
<td>• <strong>Dormant</strong></td>
</tr>
<tr>
<td></td>
<td>• <strong>Active</strong></td>
</tr>
<tr>
<td></td>
<td><strong>Note</strong>: The Dormancy Status column is only visible for 7.0 and later versions of repositories.</td>
</tr>
</tbody>
</table>

**Viewing or modifying the ACS server configuration properties**

Use these instructions to view or modify information on the ACS Server Configuration Properties page.

**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, as described in **Table 27, page 119**.
5. Click the **Projections & Stores** tab to view or modify the connection broker projections, network locations, and local stores information for the ACS server, as described in **ACS projections and stores, page 120**.
6. Click **OK** to save your changes.
7. 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 the Java Method Server from Documentum Administrator.

The *EMC Documentum Content Server Installation Guide* provides instructions on stopping and starting the Java method server.

### Table 27. ACS Server Configuration properties

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>ACS Server Configuration</strong></td>
<td></td>
</tr>
<tr>
<td>Name</td>
<td>The name that is assigned to the ACS server during the Content Server installation. The name cannot be modified.</td>
</tr>
<tr>
<td>Associated Content Server</td>
<td>The name of the Content Server the ACS server is associated with.</td>
</tr>
<tr>
<td>Description</td>
<td>A description of the ACS server.</td>
</tr>
<tr>
<td>ACS Server Version</td>
<td>The major and minor version of the ACS server.</td>
</tr>
<tr>
<td></td>
<td>The ACS server version indicates the underlying repository version.</td>
</tr>
<tr>
<td></td>
<td>Valid values:</td>
</tr>
<tr>
<td></td>
<td>• 2.1 - Specifies that the ACS server is part of a Documentum version 6.5 SPx repository.</td>
</tr>
<tr>
<td></td>
<td>• 2.2 - Specifies that the ACS server is part of a Documentum version 6.6 to 6.6 (Patch 21) repository.</td>
</tr>
<tr>
<td></td>
<td>• 2.3 - Specifies that the ACS server is part of a Documentum version 6.6 (Patch 22) to 7.2 repository.</td>
</tr>
<tr>
<td>Dormancy Status</td>
<td>Indicates the dormancy status of ACS server.</td>
</tr>
<tr>
<td></td>
<td><strong>Note:</strong> The Dormancy Status label is only visible for 7.0 and later versions of repositories.</td>
</tr>
<tr>
<td>Content Access</td>
<td>Specifies how the ACS server can access content. Valid values are:</td>
</tr>
<tr>
<td></td>
<td>• <strong>Access all stores</strong>: The ACS server can access all stores that are connected to the Content Server.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Access local stores only</strong>: The ACS server can read content from local file stores in the repository.</td>
</tr>
<tr>
<td></td>
<td>• <strong>None</strong> (disabled): The ACS server is disabled.</td>
</tr>
</tbody>
</table>

### ACS Server Connections
### Distributed Configurations

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Protocol</td>
<td>The protocol the ACS server uses. Valid values are http and https. Click <strong>Add</strong> to add a protocol, or select a protocol from the list and click <strong>Edit</strong> to modify it or <strong>Delete</strong> to remove the protocol.</td>
</tr>
<tr>
<td>Base URL</td>
<td>The base URL for the ACS server. The base URL requires the following format: <code>protocol://host:port/ACS/servlet/ACS</code></td>
</tr>
</tbody>
</table>

### ACS projections and stores

ACS projections and stores are configured on the Projections & Stores page.

**To view or modify ACS projections and stores:**

1. Connect with superuser privileges to the repository in which you want to view or modify the ACS projections and stores.
2. Select **Administration > Configuration > ACS Servers**. The ACS Servers Configurations Properties 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. Click the **Projections & Stores** tab.
5. Add or modify the information on the **Projections & Stores** page, as described in **Table 28**, page 120.
6. Click **OK** to save your changes.
7. 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 the Java Method Server from Documentum Administrator.
   - The **EMC Documentum Content Server Installation Guide** provides instructions on stopping and starting the Java method server.

### Table 28. ACS Projections & Stores properties

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Source</td>
<td>Specifies where to use projections and stores for the ACS server. Valid values are:</td>
</tr>
<tr>
<td></td>
<td>- <strong>Associated content server</strong>: The ACS server uses the connection broker projections, network locations, and local stores already configured for the associated Content Server.</td>
</tr>
</tbody>
</table>
### Distributed Configurations

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Settings entered here:</strong></td>
<td>You must enter the ACS server uses connection brokers, network locations, and near stores manually. If you select this option, an <strong>Add</strong> button displays in the Connection Broker Projections, Network Location Projections, and Local Stores sections.</td>
</tr>
</tbody>
</table>

#### Connection Broker Projections

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Target Host</td>
<td>The host name of the server that hosts the connection broker. Click <strong>Add</strong> to add a target host, or select a host from the list and click <strong>Delete</strong> to remove the host. 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.</td>
</tr>
<tr>
<td>Port</td>
<td>The port number on which the connection broker is listening.</td>
</tr>
<tr>
<td>Enabled</td>
<td>Enables projections to the connection broker.</td>
</tr>
</tbody>
</table>

#### Network Location Projections

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Network Location</td>
<td>Specifies a network location in the global registry of the Content Server host. Click <strong>Add</strong> to add a network location, or select a location from the list and click <strong>Delete</strong> to remove the location. Network locations identify locations on a network, and, optionally, a range of IP addresses, from which users connect to Documentum web clients.</td>
</tr>
<tr>
<td>Display Name</td>
<td>A name that describes the network location.</td>
</tr>
<tr>
<td>Proximity</td>
<td>The proximity value for the network location.</td>
</tr>
<tr>
<td>Enabled</td>
<td>Enables projection to that network location.</td>
</tr>
</tbody>
</table>

#### Local Stores
Distributed Configurations

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Local Store</td>
<td>A local store. Click <strong>Add</strong> to add a store, or select a store from the list and click <strong>Delete</strong> to remove the store. Local stores are defined as near to the ACS server.</td>
</tr>
<tr>
<td>Type</td>
<td>Specifies the storage type associated with the local store. This property cannot be modified.</td>
</tr>
</tbody>
</table>

## Designating connection brokers for an ACS server

Connection broker projections are configured in the Connection Broker Projections section of the ACS Server Configurations page.

**To designate a connection broker for an ACS server:**

1. Connect with superuser privileges to the repository in which you want to view or modify the connection broker.
2. Select **Administration > Configuration > ACS Servers**.
3. Select the ACS server to view or modify, select **View > Properties > Info** and click the **Projections & Stores** tab.
4. Enter the information for the connection broker, as described in [Table 29, page 122](#).
5. Click **OK**.
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 the Java Method Server from Documentum Administrator.

The *EMC Documentum Content Server Installation Guide* provides instructions on stopping and starting the Java method server.

### Table 29. ACS Connection Broker Projections properties

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
</table>
| Source      | Specifies where to use projections for the ACS server. Valid values are:  
  - **Associated content server**: The ACS server uses the connection broker projections, network locations, and local stores already configured for the associated Content Server.  
    When this option is selected, you cannot modify the connection broker projections. |
Distributed Configurations

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Settings entered here</td>
<td>Select this option to designate connection broker projections. If you select this option, an Add button displays in the Connection Broker Projections, Network Location Projections, and Local Stores sections.</td>
</tr>
</tbody>
</table>

**Connection Broker Projections**

- **Target Host**: The host name of the server that hosts the connection broker.
  - Click Add to add a target host, or select a host from the list and click Delete to remove the host.
  - 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.
- **Port**: The port number on which the connection broker is listening.
- **Enabled**: Enables projections to the connection broker.

**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 your changes.

**BOCS servers**

Branch Office Caching Services (BOCS) servers cache content locally. Caching content allow quick access to content. The amount of cached content and the storage time can be configured. Content can
also be cached programmatically prior to user requests or through a pre-caching job. A BOCS server can serve content from multiple repositories.

BOCS servers communicate only with ACS servers and DMS servers, but not directly with Content Servers. Every BOCS server for Documentum 6 or later repositories is associated with a dm_bocs_config object. The installation program for the BOCS server does not create the object at installation time. The BOCS server must be added manually, using the properties on the BOCS Servers Configuration page. All BOCS configuration objects for Documentum 6 or later repositories reside in the global registry in the /System/BocsConfig folder.

To create, modify, or view BOCS configuration objects, you must have superuser privileges and be connected to the global repository that is associated with the DFC installation. If you are not connected to the global repository and click the BOCS Server node, the system displays an error message and provides a link to the login page of the global registry repository.

Creating, viewing, or modifying BOCS servers

Use the instructions in this section to create, view, or modify the BOCS configuration object in the global registry repository after the BOCS server is installed on its host. To create, view, or modify BOCS configuration objects, you must have superuser privileges and be connected to the global registry that is associated with the DFC installation.

To create, view, or modify BOCS servers:

1. Connect to the global registry associated with the DFC installation using superuser privileges.
2. Navigate to Administration > Distributed Content Configuration > BOCS Servers.
   The BOCS Server Configurations list page appears. If you do not see the BOCS Server Configurations page, you are not connected to the global registry.
   Click Global Registry Login and connect to the correct repository.
3. Do one of the following:
   • Select File > New > BOCS Server Configuration to create a BOCS server configuration object.
   • Select a BOCS server configuration object, then select View > Properties > Info to view or modify a BOCS server configuration object.
4. Enter or modify the information on the Info and Security tabs of the New BOCS Server Configuration or BOCS Server Configuration page, as described in Table 30, page 124 and Setting BOCS server security, page 126.
5. Click Finish or OK to save your changes.

Table 30. BOCS server properties

<table>
<thead>
<tr>
<th>Field label</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>BOCS Server Configuration Info</td>
<td></td>
</tr>
<tr>
<td>Field label</td>
<td>Value</td>
</tr>
<tr>
<td>---------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Name</td>
<td>The object name of the BOCS server. The object name cannot be modified for existing BOCS server configuration objects.</td>
</tr>
<tr>
<td>Description</td>
<td>Description of the BOCS server.</td>
</tr>
<tr>
<td>BOCS Server Version</td>
<td>A numeric string that identifies the set of distributed content features with which the BOCS server is compatible. In some cases, a set of features spans multiple product versions. Valid values are:</td>
</tr>
<tr>
<td></td>
<td>• 1 - The Content Access options are limited to Read Only and None (disabled).</td>
</tr>
<tr>
<td></td>
<td>• 2.1 - Compatible with Content Server version 6.5 SPx.</td>
</tr>
<tr>
<td></td>
<td>• 2.2 - Compatible with Content Server version 6.6 to 6.6 (Patch 21).</td>
</tr>
<tr>
<td></td>
<td>• 2.3 - Compatible with Content Server versions 6.6 (Patch 22) to 7.x. This value is only valid if the actual version of the installed BOCS server is from 6.6 (Patch 22) to 7.x.</td>
</tr>
<tr>
<td>Content Access</td>
<td>Select an access type, as follows:</td>
</tr>
<tr>
<td></td>
<td>• Read and synchronous write: Select this option for the BOCS server to support read and synchronous write.</td>
</tr>
<tr>
<td></td>
<td>• Read, synchronous, and asynchronous write: Select this option for the BOCS server to support read, synchronous write, and asynchronous write.</td>
</tr>
<tr>
<td></td>
<td>• None (disabled): The BOCS server is disabled.</td>
</tr>
<tr>
<td>Network Locations</td>
<td>Network locations served by the BOCS server.</td>
</tr>
<tr>
<td></td>
<td>Click Select to access the Choose a Network Location page to select network locations.</td>
</tr>
<tr>
<td>Repositories</td>
<td>Select a repository from which to serve content, as follows:</td>
</tr>
<tr>
<td></td>
<td>• all repositories: Content is served from all repositories.</td>
</tr>
<tr>
<td></td>
<td>• selected repositories only: Serves content from all repositories that are specified on the Include list. Click Edit to add specific repositories.</td>
</tr>
<tr>
<td></td>
<td>• all except selected repositories: Serves content from all repositories except the repositories that are specified in the Exclude list.</td>
</tr>
<tr>
<td></td>
<td>Click the Edit link to add specific repositories to exclude.</td>
</tr>
</tbody>
</table>
Distributed Configurations

<table>
<thead>
<tr>
<th>Field label</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Proxy URL</td>
<td>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.</td>
</tr>
</tbody>
</table>

BOCS Server Connections

<table>
<thead>
<tr>
<th>Add</th>
<th>Click to access the BOCS Server Connection page to add a protocol and base URL for the BOCS server.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Edit</td>
<td>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.</td>
</tr>
<tr>
<td>Delete</td>
<td>To delete a BOCS server protocol and base URL, select a communication protocol and then click Delete.</td>
</tr>
</tbody>
</table>
| 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:  
 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. |

Setting BOCS server security

The BOCS server security properties specifies whether the BOCS server is in push or pull mode and is used to upload a public key from the BOCS server.

The BOCS server configuration object in the global registry contains the public key information and generates an electronic signature for the BOCS server to use when contacting the DMS server. When the BOCS server connects to the DMS server in pull or push mode, it sends its electronic signature to DMS where DMS matches the electronic signature to the public key in the BOCS configuration object. If the DMS server authenticates the BOCS electronic signature, the BOCS server can then pull or push its messages from or to the DMS server respectively.
Figure 2. New BOCS Server Configuration - Security page

To set BOCS server security:

1. Connect to the global registry associated with the DFC installation using superuser privileges.
2. Navigate to Administration > Distributed Content Configuration > BOCS Servers.
3. Do one of the following:
   - Select File > New > BOCS Server Configuration to create a BOCS server configuration object. Enter the BOCS server properties on the Info tab.
   - Select a BOCS server configuration object, then select View > Properties > Info to view or modify a BOCS server configuration object.
4. Click the Security tab and enter, view, or modify the security properties for the BOCS server, as described in Table 31, page 127.
5. Click OK to save changes.

Table 31. BOCS server security properties

<table>
<thead>
<tr>
<th>Field label</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Pull Mode Enabled</td>
<td>Specifies whether the BOCS server communicates with the DMS server using the pull mode.</td>
</tr>
<tr>
<td>Public Key Installed</td>
<td>Displays the last updated status for the public key.</td>
</tr>
<tr>
<td>Upload Public Key File</td>
<td>Click Browse to locate and install the public key file for the BOCS server.</td>
</tr>
</tbody>
</table>

Setting BOCS server communication protocols

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

To access the BOCS Server Connection page, click Add or Edit in the BOCS Server Connections section of the BOCS Server Configuration page. Creating, viewing, or modifying BOCS servers, page 124 provides the 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. Currently, the Http and Https protocols are supported.
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.

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 cannot provide content from this repository.

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 page displays.
   If the BOCS Server Configurations page does not display, you are not connected to the global registry. Click Global Registry Login and connect to the correct repository.
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.

Configuring distributed transfer settings

The distributed transfer object is created when the repository is created. The distributed transfer 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.
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 do 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 is encrypted based on what the doGetContentEncryptionMode method returns, regardless of what option you select on the Distributed Transfer Settings Properties 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 is not 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 must be created and set up in the global registry using Documentum Administrator. Administrators with superuser privileges only can configure the messaging server configuration object. Administrators with superuser privileges connecting to 6.7 and below global registry can only create default messaging server configuration object. If a messaging server configuration object exists, administrator cannot create new objects.

**Note:** You can create multiple messaging server configuration objects using Documentum Administrator 7.0 and later versions of Content Server and repositories. Use the File > New > Messaging Server Configuration in the Messaging Server list page.

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 do 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 also shows a link for the administrator to click to navigate to the login page of the global registry repository.

**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. The messaging server configuration is not visible 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**: 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.

To save time retyping existing information, you can copy a messaging server configuration using the **Save As** option. To copy a messaging server, 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 messaging server:**

1. Connect with superuser privileges to the global registry repository.

2. Select **Administration > Distributed Content Configuration > Messaging Server**.

   The Messaging Server page appears.

   **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. On the Messaging Server page, do one of the following:

   - Select a messaging server in the Name column, then select **File > Save As**.

   - Select a messaging server in the Name column and then right-click. From the available menu options, select **Save As**.

   The Messaging Server Configuration Properties page appears. The fields display the values copied from the selected messaging server; however, the **Name** field display **Copy [x] of [name]/[display name]** to keep the messaging server and display names unique.

4. Modify the properties on Info tab of the Messaging Server Configuration Properties page.
5. Click **OK** to save the changes or **Cancel** to exit without saving.
Chapter 4

User Management

This chapter contains the following topics:

- Administering users, groups, roles, and sessions, page 133
- Users, page 134
- Groups, page 148
- Roles, page 155
- Module roles, page 158
- Sessions, page 161

Administering users, groups, roles, and sessions

Users, groups, roles, and sessions are managed in the User Management node. The User Management node is accessed by selecting Administration > 🌐 User Management.

The User Management page contains links to the user management features that can be configured for a repository, as described in Table 32, page 133.

Table 32. Users, groups, roles, and sessions

<table>
<thead>
<tr>
<th>Link</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Users</td>
<td>Accesses the Users page. From the Users page you can</td>
</tr>
<tr>
<td></td>
<td>• Search for existing user accounts.</td>
</tr>
<tr>
<td></td>
<td>• Create, modify, and delete user accounts.</td>
</tr>
<tr>
<td></td>
<td>• View and assign group memberships for a particular user account.</td>
</tr>
<tr>
<td></td>
<td>• Change the home repository for particular user accounts.</td>
</tr>
</tbody>
</table>

Users, page 134 provides more information about user accounts.
<table>
<thead>
<tr>
<th>Link</th>
<th>Description</th>
</tr>
</thead>
</table>
| Groups       | Accesses the Groups page. From the Groups page you can  
• Search for existing group accounts.  
• Create, modify, and delete group accounts.  
• View and reassign group a particular group account.  
Groups, page 148 provides more information about group accounts. |
| Roles        | Accesses the Roles page. From the Roles page you can  
• Search for existing roles.  
• Create, modify, and delete roles.  
• View current group memberships and reassign roles.  
Roles, page 155 provides more information about roles. |
| Module Roles | Accesses the Modules Roles page. From the Modules Roles page you can  
• Search for existing module roles.  
• Create, modify, and delete module roles.  
• View current group memberships and reassign module roles.  
Module roles, page 158 provides more information about module roles. |
| Sessions     | Accesses the Sessions page. From the Sessions page you can  
• Search for sessions.  
• View session properties and session logs.  
Sessions, page 161 provides more information about module roles. |

**Users**

A repository user is a person or application with a user account that has been configured for a repository. User accounts are created, managed, and deleted on the User node. In a Documentum repository, user accounts are represented by user objects. Whenever a new user account is added to a repository, Content Server creates a user object. A user object specifies how a user can access a repository and what information the user can access.

**Locating users**

Use the search filters on the Users page to located users.
To locate users:

1. Connect to the repository where you want to locate a particular user.
2. Navigate to Administration > User Management > Users
   The User page displays.
3. Type information into one of more the search fields as described in Table 33, page 135.
   You can search by entering partial information, such as the first letter or a user name, group, or domain.
4. Click Search to use the search filters or click Locate All Users to display all user accounts for the repository.

Table 33. User search filters

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>User Name</td>
<td>Filters the search results by user name.</td>
</tr>
<tr>
<td>Default Group</td>
<td>Filters the search results the name of the default group.</td>
</tr>
<tr>
<td>User Login Name</td>
<td>Filters the search results by the login name of the user.</td>
</tr>
<tr>
<td>User Login Domain</td>
<td>Filters the search results by login domain.</td>
</tr>
</tbody>
</table>

Creating or modifying users

You must be the installation owner, or have system administrator or superuser privileges to create users. Superusers and system administrators cannot modify their own extended privileges.

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.

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

To create or modify user accounts:

1. Connect to the repository where you want to create new users.
2. Navigate to Administration > User Management > Users.
3. Do one of the following:
   - To create a user, select File > New > User.
     The New User page displays.
   - To modify an existing user, select the user, then select View > Properties > Info.
The User Properties page displays.

4. Enter or modify the user information, as described in Table 34, page 136.

5. Click OK.

Table 34. User properties

<table>
<thead>
<tr>
<th>Field label</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>State</td>
<td>Indicates the user account state in the repository. Valid values are:</td>
</tr>
<tr>
<td></td>
<td>• Active: The user is a currently active repository user. Active users</td>
</tr>
<tr>
<td></td>
<td>are able to connect to the repository.</td>
</tr>
<tr>
<td></td>
<td>• Inactive: The user is not currently active in the repository.</td>
</tr>
<tr>
<td></td>
<td>Inactive users are unable to connect to the repository.</td>
</tr>
<tr>
<td></td>
<td>• Locked: The user is unable to connect to the repository.</td>
</tr>
<tr>
<td></td>
<td>• Locked and inactive: The user is inactive and unable to connect</td>
</tr>
<tr>
<td></td>
<td>to the repository.</td>
</tr>
</tbody>
</table>

If the user is a superuser, only another superuser can reset the state.

Name             | The user name for the new user. The user name cannot be modified,     |
|                  |   but can be reassigned to another user.                             |
|                  |   Reassigning objects to another user, page 145 provides the more    |
|                  |   information.                                                      |

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 operating system name of the user. If the user is an     |
|                  |   LDAP user, the user login name must match the LDAP authentication   |
|                  |   name of the user.                                                 |

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.                                               |
|                  | If you are using Kerberos authentication with LDAP synchronization,  |
|                  |   the user login domain must be set to the short domain name, as     |
|                  |   described in Configuring LDAP synchronization for Kerberos users,  |
|                  |   page 109.                                                        |

User Source       | Specifies how to authenticate a given repository user’s user name    |
|                  |   and password. Valid values depend on whether the repository runs   |
|                  |   on a Linux or Windows server.                                     |
|                  | • None: The user is authenticated in a Windows domain.              |
|                  | • UNIX only: The user is authenticated using the default Linux      |
|                  |   mechanism, dm_check_password or other external password checking   |
|                  |   program.                                                         |
|                  | • Domain only: The user is authenticated against a Windows domain.  |

EMC Documentum Administrator Version 7.2 User Guide
<table>
<thead>
<tr>
<th>Field label</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>• UNIX first:</td>
<td>This is used for Linux repositories where Windows domain authentication is in use. The user is authenticated first by the default Linux mechanism; if that fails, the user is authenticated against a Windows domain.</td>
</tr>
<tr>
<td>• Domain first:</td>
<td>This is used for Linux 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 Linux mechanism.</td>
</tr>
<tr>
<td>• LDAP:</td>
<td>The user is authenticated through an LDAP directory server.</td>
</tr>
<tr>
<td>• Inline Password:</td>
<td>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.</td>
</tr>
<tr>
<td>• dm_krb:</td>
<td>The user is authenticated using Kerberos Single-Sign-On (SSO).</td>
</tr>
<tr>
<td>Password</td>
<td>The password for the user.</td>
</tr>
<tr>
<td></td>
<td>This field is displayed if Inline Password is selected as the User Source. Type the password, which is then encrypted and stored in the repository.</td>
</tr>
<tr>
<td></td>
<td>This must be provided manually for users added using an imported LDIF file.</td>
</tr>
<tr>
<td>Confirm Password</td>
<td>The password for the user.</td>
</tr>
<tr>
<td></td>
<td>This field is displayed if Inline Password is selected as the User Source. Enter the same password you entered in the Password field.</td>
</tr>
<tr>
<td>Description</td>
<td>A description of the user account.</td>
</tr>
<tr>
<td>E-Mail Address</td>
<td>The E-mail address of the user. This is the E-Mail address to which notifications are sent for workflow tasks and registered events.</td>
</tr>
<tr>
<td>User OS Name</td>
<td>The operating system user name of the user.</td>
</tr>
<tr>
<td>Windows Domain</td>
<td>The Windows domain associated with the user account or the domain on which the user is authenticated. The latter applies if Content Server is installed on a Linux host and Windows domain authentication is used.</td>
</tr>
<tr>
<td>Home Repository</td>
<td>The repository where the user receives notifications and tasks.</td>
</tr>
<tr>
<td>User is global</td>
<td>If the user is created in the governing repository of a federation, select this option to propagate the user account to all members of the federation.</td>
</tr>
<tr>
<td>Field label</td>
<td>Value</td>
</tr>
<tr>
<td>-----------------------------------</td>
<td>----------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Restrict Folder Access To</td>
<td>Specifies which folders the user can access. Click <strong>Select</strong> to specify a cabinet or folder. Only the selected cabinets and folders display for the user. The other folders do not display but the user can access the folders using the search or advanced search options. If no folders or cabinets are specified, the user has access to all folders and cabinets in the repository, depending on the permissions on those cabinets and folders, and depending on folder security.</td>
</tr>
<tr>
<td>Default Folder</td>
<td>The default storage place for any object the user creates. This option only displays when you are creating a user. Valid values are:</td>
</tr>
<tr>
<td></td>
<td>• <strong>Choose existing folder</strong>: Select this option to assign a folder you already created as the default folder for that user.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Choose/Create folder with the user name</strong>: Select this option to automatically create a folder with the name of the user as the object name.</td>
</tr>
<tr>
<td>Default Group</td>
<td>The group that is associated with the default permission set of the user. Click <strong>Select</strong> to specify a default group. When the user creates an object in the repository, it automatically belongs to this group.</td>
</tr>
<tr>
<td>Default Permission Set</td>
<td>The permission set that assigns the default permissions to objects the user creates. Click <strong>Select</strong> to specify a default permission set.</td>
</tr>
<tr>
<td>Db Name</td>
<td>The user name of the user in the underlying RDBMS. The DB Name is only required if the user is a repository owner or a user who registers RDBMS tables.</td>
</tr>
<tr>
<td>Privileges</td>
<td>The privileges that are assigned to the user. User privileges authorize certain users to perform activities in the repository. Select one of the privileges from the drop-down list, as follows:</td>
</tr>
<tr>
<td>Field label</td>
<td>Value</td>
</tr>
<tr>
<td>----------------------</td>
<td>----------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td></td>
<td>• Superuser: If you grant superuser privileges to a user, add that user manually to the group called admingroup. If you revoke a user’s</td>
</tr>
<tr>
<td></td>
<td>superuser privileges, remove the user from the admingroup.</td>
</tr>
<tr>
<td>Extended Privileges</td>
<td>Specifies the auditing privileges for the user. Superusers and system administrators cannot modify their own extended privileges.</td>
</tr>
<tr>
<td></td>
<td>• None: The user cannot configure auditing, view audit trails, or purge audit trails.</td>
</tr>
<tr>
<td></td>
<td>• Config audit: The user can configure auditing.</td>
</tr>
<tr>
<td></td>
<td>• Purge audit: The user can purge existing audit trails.</td>
</tr>
<tr>
<td></td>
<td>• Config and Purge Audit: The user can configure auditing and purge existing audit trails.</td>
</tr>
<tr>
<td></td>
<td>• View Audit: The user can view audit trails.</td>
</tr>
<tr>
<td></td>
<td>• Config and View Audit: The user can configure auditing and view existing audit trails.</td>
</tr>
<tr>
<td></td>
<td>• View and Purge Audit: The user can view existing audit trails and purge them.</td>
</tr>
<tr>
<td></td>
<td>• Config, View, and Purge Audit: The user can configure auditing and view and purge existing audit trails.</td>
</tr>
<tr>
<td>Client Capability</td>
<td>Describes the expertise level of the user.</td>
</tr>
<tr>
<td></td>
<td>The client capability setting is used by Documentum client products to determine which functionality to deliver to the user. Content</td>
</tr>
<tr>
<td></td>
<td>Server does not recognize or use the client capability setting. For information about the client features available with each setting,</td>
</tr>
<tr>
<td></td>
<td>refer to the Documentum client documentation.</td>
</tr>
<tr>
<td></td>
<td>Choose a user type from the list:</td>
</tr>
<tr>
<td></td>
<td>• Consumer</td>
</tr>
<tr>
<td></td>
<td>• Contributor</td>
</tr>
<tr>
<td></td>
<td>• Coordinator</td>
</tr>
<tr>
<td></td>
<td>• System Administrator</td>
</tr>
<tr>
<td>Alias Set</td>
<td>The default alias set for the user. Click Select to specify an alias set.</td>
</tr>
<tr>
<td>Disable Workflow</td>
<td>Indicates whether a user can receive workflow tasks.</td>
</tr>
<tr>
<td>Disable Authentication Failure Checking</td>
<td>If selected, user can exceed the number of failed logins specified in the Maximum Authentication Attempts field of the repository configuration object.</td>
</tr>
</tbody>
</table>
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 or modifying users, page 135 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.

Setting default permissions for folders and cabinets

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 default folder or creating a folder with the user’s name. If you have Documentum Administrator create the folder for a new user and you can control the permissions assigned to folder.

To set default permissions for folders:

1. Create a 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 alias to the user who owns the permission set you use for the DefaultFolderAcl alias.

When you add a user, Documentum Administrator applies the permission set you designate to the new folder. 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 folder 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 default folder for an existing user and permissions on the set are applied if you have created the necessary alias set and aliases.

If the UserPropertiesConfiguration alias set does not exist and a superuser creates the user, the user owns the folder and has delete permission. If a system administrator creates the 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.
Importing users

You can create repository users from information contained in an input file. Before you begin importing users, determine the following:

- **Authentication type**
  
  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.

- **Groups and ACLs**
  
  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.

- **Passwords**
  
  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 by modifying the user account after the user has been imported.

**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.
5. Select File > Import Users.
   
   The Import User page displays.
6. Enter the user information, as described in Table 35, page 141.
7. Click Finish.

**Table 35. Import user properties**

<table>
<thead>
<tr>
<th>Field label</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>State</strong></td>
<td>Indicates the user’s state in the repository. Select one of the following:</td>
</tr>
<tr>
<td></td>
<td>• <strong>Active</strong>: The user is a currently active repository user. Active users are able to connect to the repository.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Inactive</strong>: The user is not currently active in the repository. Inactive users are unable to connect to the repository.</td>
</tr>
<tr>
<td></td>
<td>If the user is a superuser, only another superuser can reset the state.</td>
</tr>
<tr>
<td><strong>Source</strong></td>
<td>The name of an input file. Click <strong>Browse</strong> to browse to the location of the LDIF file containing information for creating the new users.</td>
</tr>
<tr>
<td></td>
<td><strong>Import file format, page 144</strong> provides more information about the LDIF file format.</td>
</tr>
<tr>
<td>Field label</td>
<td>Value</td>
</tr>
<tr>
<td>-------------------</td>
<td>----------------------------------------------------------------------</td>
</tr>
<tr>
<td>User Source</td>
<td>Specifies how to authenticate a given repository user’s user name and password. Valid values are:</td>
</tr>
<tr>
<td></td>
<td>• <strong>None</strong>: Windows only. This means the user is authenticated in a Windows domain.</td>
</tr>
<tr>
<td></td>
<td>• <strong>UNIX only</strong>: The user is authenticated using the default Linux mechanism, dm_check_password or other external password checking program. This option only displays on Linux hosts.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Domain only</strong>: The user is authenticated against a Windows domain. This option only displays on Linux hosts.</td>
</tr>
<tr>
<td></td>
<td>• <strong>UNIX first</strong>: This is used for Linux repositories where Windows domain authentication is in use. This option only displays on Linux hosts.</td>
</tr>
<tr>
<td></td>
<td>The user is authenticated first by the default Linux mechanism. If the authentication fails, the user is authenticated against a Windows domain.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Domain first</strong>: This is used for Linux repositories where Windows domain authentication is in use. This option only displays on Linux hosts.</td>
</tr>
<tr>
<td></td>
<td>The user is authenticated first against a Windows domain; if that fails, the user is authenticated by the default Linux mechanism.</td>
</tr>
<tr>
<td></td>
<td>• <strong>LDAP</strong>: The user is authenticated through an LDAP directory server.</td>
</tr>
<tr>
<td>Description</td>
<td>A description of the user account.</td>
</tr>
<tr>
<td>E-Mail Address</td>
<td>The E-mail address of the user. This is the E-Mail address to which notifications are sent for workflow tasks and registered events.</td>
</tr>
<tr>
<td>Windows Domain</td>
<td>(Windows only.) The domain name associated with the new user’s Windows account.</td>
</tr>
<tr>
<td>Home Repository</td>
<td>The repository where the user receives notifications and tasks.</td>
</tr>
<tr>
<td>User is global</td>
<td>If the user is created in the governing repository of a federation, select this option to propagate the user account to all members of the federation.</td>
</tr>
<tr>
<td>Default Folder</td>
<td>The default storage place for any object the user creates. Click <strong>Select</strong> to assign a folder.</td>
</tr>
<tr>
<td>Default Group</td>
<td>The group that is associated with the default permission set of the user. Click <strong>Select</strong> to specify a default group.</td>
</tr>
<tr>
<td></td>
<td>When the user creates an object in the repository, it automatically belongs to this group.</td>
</tr>
<tr>
<td>Default ACL</td>
<td>The permission set that assigns the default permissions to objects the user creates. Click <strong>Select</strong> to specify a default permission set.</td>
</tr>
<tr>
<td>Field label</td>
<td>Value</td>
</tr>
<tr>
<td>---------------------</td>
<td>----------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Db Name</td>
<td>The user name of the user in the underlying RDBMS. The DB Name is only required if the user is a repository owner or a user who registers RDBMS tables.</td>
</tr>
<tr>
<td>Privileges</td>
<td>The privileges that are assigned to the user.</td>
</tr>
<tr>
<td></td>
<td>User privileges authorize certain users to perform activities in the repository. Select one of the privileges from the drop-down list, as follows:</td>
</tr>
<tr>
<td></td>
<td>• None</td>
</tr>
<tr>
<td></td>
<td>• Create Type</td>
</tr>
<tr>
<td></td>
<td>• Create Cabinet</td>
</tr>
<tr>
<td></td>
<td>• Create Cabinet and Type</td>
</tr>
<tr>
<td></td>
<td>• Create Group</td>
</tr>
<tr>
<td></td>
<td>• Create Group and Type</td>
</tr>
<tr>
<td></td>
<td>• Create Group and Cabinet</td>
</tr>
<tr>
<td></td>
<td>• Create Group, Cabinet and Type</td>
</tr>
<tr>
<td></td>
<td>• System Administrator</td>
</tr>
<tr>
<td></td>
<td>• 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.</td>
</tr>
<tr>
<td>Client Capability</td>
<td>Indicates what expertise level of the user. This option is for informative purposes only and is not associated with any privileges. Content Server does not recognize or enforce these settings.</td>
</tr>
<tr>
<td></td>
<td>Choose a user type from the list:</td>
</tr>
<tr>
<td></td>
<td>• Consumer</td>
</tr>
<tr>
<td></td>
<td>• Contributor</td>
</tr>
<tr>
<td></td>
<td>• Coordinator</td>
</tr>
<tr>
<td></td>
<td>• System Administrator</td>
</tr>
<tr>
<td>Alias Set</td>
<td>The default alias set for the user. Click Select to specify an alias set.</td>
</tr>
<tr>
<td>If user exists, then overwrite user information</td>
<td>Select this option if a user already exists in the repository and you want to replace existing information with the imported information.</td>
</tr>
<tr>
<td>If user exists, then ignore information</td>
<td>Select this option if a user already exists in the repository and you want to retain the existing information.</td>
</tr>
</tbody>
</table>
Import file format

You can create repository users from information contained in an input file.

Each imported user 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 36. Default values for new users

<table>
<thead>
<tr>
<th>Argument</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td>user_login_name</td>
<td>username</td>
</tr>
<tr>
<td>privileges</td>
<td>0 (None)</td>
</tr>
<tr>
<td>folder</td>
<td>/username</td>
</tr>
<tr>
<td>group</td>
<td>docu</td>
</tr>
<tr>
<td>client_capability</td>
<td>1</td>
</tr>
</tbody>
</table>

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)
faulted_auth_attempt (set to integer value)
You can specify as many of the 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 creates the default folder for each user if it does not already exist.

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 users 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 objects to another user, use the instructions in Reassigning objects to another user, page 145.

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.
4. Click Finish.

Reassigning objects to another user

If you want to delete a user from the repository, make the user inactive, or rename a user, you can assign objects owned by that user to another user. For example, to change the user name of a particular user, you have to create a new user and assign the objects that belonged to the old user name to the new user.

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 User page:
   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.
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**.

**Activating or deactivating a user account**

Changing a user account from active to inactive is an alternative to deleting the user from the repository. If the account is a superuser account, only another superuser can reset the account.

**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**.
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 completed
   You 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. **Dynamic groups, page 149** provides more information on dynamic groups.

To create or modify groups, you must have privileges as shown in the following table:

<table>
<thead>
<tr>
<th>Privilege</th>
<th>Create</th>
<th>Modify</th>
<th>Delete</th>
</tr>
</thead>
<tbody>
<tr>
<td>Create Group</td>
<td>Can create group or assign ownership to a group to which the user belongs.</td>
<td>Can add or delete members and assign ownership to a group to which the user belongs.</td>
<td>Can delete groups the user owns, including groups where a group is owner and the user is a member of the group.</td>
</tr>
<tr>
<td>System administrator</td>
<td>Can create group or assign ownership to a group to which the user belongs.</td>
<td>Can update the group the system administrator owns, including groups where a group is owner and the system administrator is a member of the group.</td>
<td>Can delete groups the system administrator owns, including groups where a group is owner and the system administrator is a member of the group.</td>
</tr>
<tr>
<td>Superuser</td>
<td>Can create a group and assign ownership to a different user or group.</td>
<td>Can update group administrator, owner, or members of a group.</td>
<td>Can delete any group.</td>
</tr>
</tbody>
</table>

A group can own SysObjects and permission sets.
The name assigned to a group must consist of characters that are compatible with the Content 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 name.

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 can 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.

Privileged groups

Installing Content Server installs a set of privileged groups. Members of privileged are allowed to perform privileged operations even though the members do not have the privileges as individuals. The privileged groups are divided into two sets.

The first set of privileged groups are used in applications or for administration needs. With two exceptions, these privileged groups have no default members when they are created. You must populate the groups. The following table describes these groups.
Table 38. Privileged groups

<table>
<thead>
<tr>
<th>Group</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>dm_browse_all</td>
<td>Members of this group can browse any cabinets and folders in the repository, folders except the rooms that were created using Documentum Collaborative Services (DCS). The dm_browse_all_dynamic is a member of this group by default.</td>
</tr>
<tr>
<td>dm_browse_all_dynamic</td>
<td>This is a dynamic role group whose members can browse any object in the repository. The dm_browse_all_dynamic group is a member of the dm_browse_all group.</td>
</tr>
<tr>
<td>dm_escalated_allow_save_on_lock</td>
<td>Used internally for RPS.</td>
</tr>
<tr>
<td>dm_retention_managers</td>
<td>Members of this group can:</td>
</tr>
<tr>
<td></td>
<td>• Own retainer objects (representing retention policies)</td>
</tr>
<tr>
<td></td>
<td>• Add and remove a retainer from any SysObject.</td>
</tr>
<tr>
<td></td>
<td>• Add and remove content in a retained object</td>
</tr>
<tr>
<td></td>
<td>• Change the containment in a retained virtual document</td>
</tr>
<tr>
<td></td>
<td>This is a non-dynamic group.</td>
</tr>
<tr>
<td>dmRetention_users</td>
<td>Members of this group can add retainers (retention policies) to SysObjects.</td>
</tr>
<tr>
<td></td>
<td>This is a non-dynamic group.</td>
</tr>
<tr>
<td>dm_superusers</td>
<td>Members of this group are treated as superusers in the repository. The dm_superusers_dynamic group is a member of this group by default.</td>
</tr>
<tr>
<td>dm_superusers_dynamic</td>
<td>A dynamic role group whose members are treated as superusers in the repository. The dm_superusers_dynamic group is a member of the dm_superusers group.</td>
</tr>
<tr>
<td>dm_sysadmin</td>
<td>Members of this group are treated as users with system administrator user privileges.</td>
</tr>
<tr>
<td>dm_create_user</td>
<td>Member of this group have Create User user privilege.</td>
</tr>
<tr>
<td>dm_create_type</td>
<td>Member of this group have Create Type user privilege.</td>
</tr>
<tr>
<td>dm_create_group</td>
<td>Member of this group have Create Group user privilege.</td>
</tr>
<tr>
<td>dm_create_cabinet</td>
<td>Member of this group have Create Cabinet user privilege.</td>
</tr>
</tbody>
</table>

The second set of privileged groups are privileged roles that are used internally by DFC. You cannot add or remove members from these groups. The groups are:

• dm_assume_user
• dm_datefield_override
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.
   The Groups page displays the first ten groups in the repository.
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 group memberships

Use these instructions to see where a group is used.

To view group memberships:
1. Select the correct group.
2. Select View > View Current Group Memberships.

Creating, viewing, or modifying groups

You can create a group or view and modify group properties on the Info tab of the New Group and Group properties pages.
To create, view, or modify groups:

1. Navigate to Administration > User Management > Groups.
   The Groups page displays.

2. Do one of the following:
   - Select File > New > Group to create a group.
   - Select an existing group from the list and select View > Properties > Info to view or modify the properties of the group.

3. Enter or modify information on the Info tab of the New Group page or Group Properties page, as described in Table 39, page 152.

4. Click OK to save your changes.

Table 39. Group properties

<table>
<thead>
<tr>
<th>Field label</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>The name of the repository group.</td>
</tr>
<tr>
<td>Group Native Room</td>
<td>The group's native room. This field appears only if the rooms feature of Collaborative Services is enabled.</td>
</tr>
<tr>
<td>E-Mail Address</td>
<td>The email address for the new group. If no value is entered in this field, the group email address defaults to the group name.</td>
</tr>
<tr>
<td>Owner</td>
<td>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.</td>
</tr>
<tr>
<td>Administrator</td>
<td>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. Only a superuser and the group owner can change the administrator of a group.</td>
</tr>
<tr>
<td>Alias Set</td>
<td>The default alias set for the group.</td>
</tr>
<tr>
<td>Group is Global</td>
<td>Displayed only in the governing repository of a federation and the group must be a global group.</td>
</tr>
<tr>
<td>Description</td>
<td>A description of the group.</td>
</tr>
<tr>
<td>Field label</td>
<td>Value</td>
</tr>
<tr>
<td>-------------</td>
<td>-------</td>
</tr>
<tr>
<td>Private</td>
<td>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.</td>
</tr>
<tr>
<td>Dynamic</td>
<td>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. Dynamic groups, page 149 provides more information on dynamic groups.</td>
</tr>
<tr>
<td>Protected</td>
<td>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. The Protected checkbox is enabled only when Dynamic Group is selected.</td>
</tr>
</tbody>
</table>

## 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 page.
2. Double-click the name of the group to which you want to add users and then select File > Add Members.
3. To jump to a particular user, group, or role, type the name in the text box and click Go, or filter the list using one of the predefined filters from the drop-down list.
4. Select the names of the users, groups, or roles you are adding to the group.

5. Click the right arrow.
   The members are moved to the right-hand side of the page.

6. Click OK.

Removing users from a group

Use these instructions to remove users from a group.

To remove users from a group:
1. Navigate to Administration > User Management > Groups to access the Groups page.
2. Double-click the group from which you want to delete users.
3. Select the names of the users you are deleting from the group.
4. 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 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 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.

**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.

If you create a role as a domain, it is listed in the groups list, not the roles list.

**Creating, viewing, or modifying roles**

Use these instructions to create, view, or modify roles.

**To create roles:**

1. Navigate to **Administration > User Management > Roles**.
   The Roles page displays.
2. Do one of the following:
   • Select **File > New > Role** to create a role.
   • Select a group, then select **View > Properties > Info** to view or modify the properties of the role.
3. Enter or modify information on the Info tab of the **New Role** page or **Role Properties** page,
   as described in **Table 40, page 156**.
4. Click **OK** to save your changes.
### Table 40. Role properties

<table>
<thead>
<tr>
<th>Field label</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>The name of the repository role.</td>
</tr>
<tr>
<td>Group Native Room</td>
<td>The native room for the role. The field appears only if the rooms feature of Collaborative Services is enabled.</td>
</tr>
<tr>
<td>E-Mail Address</td>
<td>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.</td>
</tr>
<tr>
<td>Owner</td>
<td>The name of a repository user who has the Create Group privilege and who owns this role.</td>
</tr>
<tr>
<td>Administrator</td>
<td>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.</td>
</tr>
<tr>
<td>Alias Set</td>
<td>The default alias set for the role.</td>
</tr>
<tr>
<td>Role Is Global</td>
<td>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.</td>
</tr>
<tr>
<td>Description</td>
<td>A description of the role.</td>
</tr>
<tr>
<td>Private</td>
<td>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.</td>
</tr>
<tr>
<td>Create role as domain</td>
<td>Select to create a dm_group object with group_class as domain. This field only appears on the New Role - Info page.</td>
</tr>
</tbody>
</table>
### 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.
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.
4. Click OK.

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.
Creating, viewing, or modifying module roles

Use these instructions to create new module roles.

To create, view, or modify module roles:

1. Navigate to Administration > User Management > Module Roles .
   The Module Roles page displays.

2. Do one of the following:
   - Select File > New > Module Role to create a module role.
   - Select a module role, then select View > Properties > Infor to view or modify the properties of the module role.

3. Enter or modify the information on Info tab of the New Module Role - Info page or the Module Role Properties page, as described in Table 41, page 159.

4. Click OK to save your changes.

Table 41. Module role properties

<table>
<thead>
<tr>
<th>Field label</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>The name of the repository module role.</td>
</tr>
<tr>
<td>Group Native Room</td>
<td>The native room for the module role. The field appears only if the rooms feature of Collaborative Services is enabled.</td>
</tr>
<tr>
<td>E-Mail Address</td>
<td>The email address for the module role.</td>
</tr>
<tr>
<td></td>
<td>If no value is entered in this field, the module role email address defaults to the module role name.</td>
</tr>
<tr>
<td>Owner</td>
<td>The name of a repository user who has the Create Group privilege and who owns this module role.</td>
</tr>
<tr>
<td>Administrator</td>
<td>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.</td>
</tr>
<tr>
<td>Alias Set</td>
<td>The default alias set for the module role.</td>
</tr>
<tr>
<td>Module Role is Global</td>
<td>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.</td>
</tr>
<tr>
<td>Description</td>
<td>A description of the module role.</td>
</tr>
</tbody>
</table>
**Field label**  | **Value**
--- | ---
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 role 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 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.

---

**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.

**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**.

**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 the **>>**.

**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 42. Session information**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Root Process Start Date</td>
<td>The last start date for the server to which the session is connected</td>
</tr>
<tr>
<td>Root Process ID</td>
<td>The process ID of the server on its host</td>
</tr>
<tr>
<td>User Name</td>
<td>The session user</td>
</tr>
<tr>
<td>Client Host</td>
<td>The host from which the session is connected</td>
</tr>
<tr>
<td>Session ID</td>
<td>The ID of the current repository session</td>
</tr>
<tr>
<td>Database Session ID</td>
<td>The ID of the current database session</td>
</tr>
<tr>
<td>Session Process ID</td>
<td>The operating system ID of the current session process</td>
</tr>
<tr>
<td>Start Time</td>
<td>The time the session was opened</td>
</tr>
<tr>
<td>Last Used</td>
<td>The time of the last activity for the session</td>
</tr>
<tr>
<td>Session Status</td>
<td>The status of the current session</td>
</tr>
<tr>
<td>Client Library Version</td>
<td>The DMCL version in use</td>
</tr>
<tr>
<td>User Authentication</td>
<td>The authentication type</td>
</tr>
<tr>
<td>Shutdown Flag</td>
<td>An internal flag</td>
</tr>
<tr>
<td>Client Locale</td>
<td>The preferred locale for repository sessions started during an API session</td>
</tr>
</tbody>
</table>

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.
Chapter 5

Security

This chapter contains the following topics:

- Permission sets, page 165

Permission sets

Permission sets are displayed on the Permission Sets page and are accessed by selecting Administration > Security. The Permission Sets page displays all permission sets that are configured for the repository, as described in Table 43, page 165.

Table 43. Permissions Sets page

<table>
<thead>
<tr>
<th>Column</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>The object name of the permission set.</td>
</tr>
<tr>
<td>Owner</td>
<td>The user or group that owns the permission set.</td>
</tr>
<tr>
<td>Class</td>
<td>Specifies set how the permission set is used:</td>
</tr>
<tr>
<td></td>
<td>• Regular: The permission set can only be used by the owner.</td>
</tr>
<tr>
<td></td>
<td>• Public: The permission set can be used by any user.</td>
</tr>
<tr>
<td>Description</td>
<td>A description of the permission set.</td>
</tr>
</tbody>
</table>

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.

**Creating, viewing, or modifying permission sets**

Use the instructions in this section to create new permission sets.

**To create, view, or modify a permission set:**

1. Navigate to **Administration > Security**.
   The **Permission Sets** list page appears.

2. Do one of the following:
   • Select **File > New > Permission Set** to create a permission set.
   • Select a permission set, the select **View > Properties > Info** to view or modify the properties of the permission set.

3. Enter the properties on the Info tab of the **New Permission Set - Info** or view and modify properties on the Info tab of the Permission Sets Properties page, as described in **Table 44**, page 166.

4. Enter the properties on the Permissions tab of the **New Permission Set - Info** or view and modify properties on the Permissions tab of the **Permission Sets Properties** page, as described in **Table 45**, page 167.

5. Click **OK** to save your changes.
   Before the permission set is saved, Content Server validates the permission set, as described in **Permission set validation**, page 174.

**Table 44. Permission set properties**

<table>
<thead>
<tr>
<th><strong>Field label</strong></th>
<th><strong>Value</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>The name of the permission set.</td>
</tr>
<tr>
<td>Description</td>
<td>A description of the permission set.</td>
</tr>
</tbody>
</table>
| Owner          | Indicates who owns the permission set.
  • 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. |
| Is Internal    | Specifies whether the permission set is implicitly created by the server (T) or explicitly created by the user (F). |
Field label | Value
--- | ---
Class | Specifies the class for the permission set. Valid values are:
- **Regular**: Only the user or group who creates the permission set can use it. Any user or group in the repository except the repository owner can create a Regular permission set.
- **Public**: The 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.

Globally Managed | If the permission set is being created in the governing repository of a federation, select to propagate the attributes to all members of the federation.

### Adding, viewing, or modifying permissions for a permission set

Permissions are added, viewed, or modified on the Permissions tab of the New Permission Set - Info or the Permissions tab of the Permission Sets Properties page, as described in Table 45, page 167.

#### Table 45. Permission properties

<table>
<thead>
<tr>
<th>Field label</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Required Groups</td>
<td>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 <strong>Add</strong> 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 <strong>Remove</strong> to remove a required group.</td>
</tr>
<tr>
<td>Group</td>
<td>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 <strong>No Required Groups exist for the permission set.</strong></td>
</tr>
</tbody>
</table>
Security

<table>
<thead>
<tr>
<th>Field label</th>
<th>Value</th>
</tr>
</thead>
</table>
| 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.                                                                                                                                   |
| 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         | 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.  
• Click **Add** to add users or groups and their permissions for the permission set.                                                                                                            |
|                         | • 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                | If there are validation conflicts, the system displays reasons for the conflicts. For example:                                                                                                      |
|                         | • **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 | 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.

- 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.

---

### Copying a permission set

Use the instructions in this section to copy a permission set. You can only copy a permission set if you are connected as a superuser. The **File > Save As...** option only displays for 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.

### 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 displays.
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 displays.
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.
      - 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.
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.

Deleting a permission set

Use these instructions to delete permission sets.

To delete a permission set:
1. Navigate to Administration > Security.
2. Select the permission sets to delete.
4. Click OK.

Assigning basic and extended object permissions

On the Set Access Permissions page, set the basic and extended permissions for a user.

To assign 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 object.

- **Browse**
  Users can view the properties but not the content of the object.

- **Read**
  Users can view both the properties and content of the object.

- **Relate**
  Users can browse, read, and add annotations to the object.

- **Version**
  Users can browse, read, relate, and they can modify the content of the object. Users can check in a new version of the object (with a new version number). Users cannot overwrite an existing version or edit object properties.

- **Write**
  Users can browse, read, relate, version, and they can edit object properties and check in the object as the same version.

- **Delete**
  Users can browse, read, relate, version, write, and delete items.

2. To assign extended permissions to a user, 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 object 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 object with a lifecycle applied to it.

   - **Change Permission**
     Users with Change Permissions can modify the basic permissions of an object.

   - **Change Ownership**
     Users with Change Ownership permissions can change the owner of the object. 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, a user is allowed to delete documents but not to 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.

### Permission set associations

Use the instructions in this section to locate the objects that use a particular permission set.

**To view permission set associations:**

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 objects or users who use the permission set, select that object type from the list.

### Changing the permissions assigned to a user

Use the instructions in this section to change user permissions in a permission set.

**To change the permissions of a user:**

1. Navigate to **Administration > Security**.
   The **Permission Sets** list page displays.
2. Select the permission set to modify and then click **View > Properties > Info**.
   The Info page displays.
3. Click the **Permissions** tab.
   The Permissions page displays.
4. In the **Grant access to** section, select the users to modify.
5. Click **Edit**.
   The **Set Access Permission** page displays.
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 validation

Content Server validates permission sets before a permission set is saved, as follows:

- 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.

- 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.

If Trusted Content Services is enabled, the Content Server performs the following additional validations:

- 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.

- 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.

- 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.
Chapter 6

Audit Management

This chapter contains the following topics:

• Auditing, page 175
• Auditing by object type, page 176
• Auditing by object instance, page 178
• Auditing by events selected for all objects in the repository, page 179
• Search audit, page 180
• Audit policies, page 181
• Registering audits, page 183
• Adding, modifying, or removing audits, page 184
• Verifying or purging audit trails, page 184

Auditing

Auditing is a security feature for monitoring events that occur in a repository or application. Auditing an event creates an audit trail, a history in the repository of the occurrence of the event. Audit information can be used to:

• Analyze patterns of access to objects.
• Monitor when critical documents change or when the status of a critical document changes.
• Monitor the activity of specific users.
• Record all occurrences of a particular event on a given object or given object type
• Record all occurrences of a particular event in the repository, regardless of the object to which it occurs
• Record all workflow-related events in the repository
• Record all occurrences of a particular workflow event for all workflows started from a given process definition
• Record all executions of a particular job
• Record all events in the repository
Note: Audit management requires extended user privileges.

Auditing is managed on the Audit Management page, which can be accessed by selecting Administration > Audit Management. The Audit Management page contains links to the following auditing features:

- Auditing by object type, page 176
- Auditing by object instance, page 178
- Auditing by events selected for all objects in the repository, page 179
- Search audit, page 180
- Audit policies, page 181

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 add, modify, or delete 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. The objects locator displays the aspect types along with the existing standard types. To audit the object instances with aspect attributes, register the related aspect type for auditing.

3. Select a type to audit, then click OK.
   The Register Audit page displays with the selected object type.

4. Do one of the following:
   - To add an audit, click Add Audit.
     A more detailed Register Audit page displays. Specify the audit criteria and audit events for the object, as described in Table 46, page 177.
   - To edit an audit, select the object name and click Edit.
     A more detailed Register Audit page displays. Specify the audit criteria and audit events for the object, as described in Table 46, page 177.
   - To remove an audit, select the object name and click Unaudit.

5. Click OK to save your changes.
Table 46. Object auditing properties

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
</table>
| Application Code   | Enter the application code to audit only objects with a particular application code.  
The application code is a property set by the client application that creates the object. For example, an application sets the application code to the value Internal. To audit objects of the type you selected with application code Internal, type **Internal** in the Application Code field.  
You cannot enter a value in the field if you previously selected a dm_user, dm_acl, or dm_group object type. |
| Lifecycle          | Records objects that are attached to a lifecycle. Click **Select Lifecycle** to access the **Choose a lifecycle** page. Select the correct lifecycle and then click **OK**. |
| State              | Records only those objects attached to the lifecycle and in a particular state. Select a state from the drop-down list.                        |
| Attributes         | Records the values of particular properties of the object in the audit trail. Click **Select Attributes** to access the **Choose an attribute** page.  
Select the properties whose values you want to record, click >, then click **Add**. To remove any properties, select them on the right-hand side of the page and click <.  
Click **OK** when you are finished. |
| Has signature      | Select to sign the audit trail.                                                                                                                                                                      |
| manifested         |                                                                                                                                                                                                         |
| Include all subtypes | Select to include all subtypes of the audited object type.                                                                                                                                  |
| Authentication      | Select to require authentication for custom (user-defined) events that are audited.                                                                                                               |
| required            |                                                                                                                                                                                                         |
| Add                 | Click to access the **Choose an event** page and select the events you want to register.                                                                                                             
Select one or more events to audit and click > to move the events to the Selected Items column. To remove any events, select them in the Selected Items column and click <. Click **OK** when you are finished.  
To unregister any events, select them in the Event Name list and click **Remove**. |

### Choosing a type

On this page, select a type and then click **OK** to accept the type or **Cancel** to cancel the action.
Auditing by object instance

Auditing by object instance creates audit trails for events for a particular object in the repository. You can set audits only for one object type at a time.

Aspect attributes can be audited if they are attached to SysObject, user, group, and acl objects, and any of their associated subtypes. Auditing aspect attributes requires that the related aspect type is registered for auditing.

You must have Config Audit privileges to audit object instances.

To add, modify, or delete auditing by object instance:

1. Connect to the repository and navigate to Administration > Audit Management.
   The Audit Management list page displays.
2. Click Manage Auditing by Object Instance.
   The Choose Objects page displays.
3. Select one or more objects to audit, 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. Click OK.
   The Register Audit page displays with the selected object instances 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. Do one of the following:
   • To add or edit an audit, select the object instance and click Edit.
     A more detailed Register Audit page displays.
     The following fields are disabled:
     — Application Code
     — Lifecycle
     — State
     — Has signature manifested
     — Include all subtypes
     — Authentication Required
     These fields are enabled only for auditing by object type.
     Note: The Add Audit button is disabled for object instance.
   • To remove an audit, select the object instance and click Unaudit.
6. Click OK.
Table 47. Object instance auditing properties

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Attributes</td>
<td>Records the values of particular properties of the object in the audit trail. Click Select Attributes to access the Choose an attribute page. Select the properties whose values you want to record, click &gt;, then click Add. To remove any properties, select them on the right-hand side of the page and click &lt;. Click OK when you are finished.</td>
</tr>
<tr>
<td>Add</td>
<td>Click to access the Choose an event page and select the events you want to register. Select one or more events to audit and click &gt; to move the events to the Selected Items column. To remove any events, select them in the Selected Items column and click &lt;. Click OK when you are finished. To unregister any events, select them in the Event Name list and click Remove.</td>
</tr>
</tbody>
</table>

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 add or remove auditing by events:

1. Connect to the repository and navigate to Administration > Audit Management. The Audit Management list page displays.
2. Click Manage Auditing by events selected for all objects in the repository. The Register Audit page displays. 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. Do one of the following:
   • To add an event, click Add.
     The Choose an event page displays. Select the events to audit, then click to move the events to the Selected Items column. Click OK to save your changes.
   • To remove an event, select the event, then click Remove.

4. Click OK.

Search audit

The Search Audit feature lets you search and view audit trails. You must have View Audit extended privileges to search for and view existing audit trails.

To search and 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. Enter the search criteria, as described in Table 48, page 180.
4. 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.
5. To view the properties of an audit trail, select the audit trail, then click View > Properties > Info.
6. To return to the Audit Management list page, click the Audit Management link at the top of the page.

Table 48. Audit search properties

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Search By</td>
<td>Indicates whether to use the criteria specified on the search page or a DQL query to search for the audit trail.</td>
</tr>
<tr>
<td></td>
<td>Do one of the following:</td>
</tr>
<tr>
<td></td>
<td>• Select the Search criteria defined below option and enter the search criteria.</td>
</tr>
<tr>
<td></td>
<td>• Select the DQL option and enter a DQL query in the Where Clause field. Click OK to display the query results.</td>
</tr>
<tr>
<td>Events</td>
<td>Restricts the search by events. Click Select and select one or more events and click OK.</td>
</tr>
</tbody>
</table>
Audit policies

An audit policy ensures that only the users or groups that are specified in the purge policy can delete an audit record. If an unauthorized user or group attempts to delete the audit record, Content Server throws an error message. If there are multiple policies for same user, the policy with the highest permissions is in effect.

Audit policies specify which user, group, or role can purge audit trails. You must be an Install Owner to access and manage audit policies. Other users can only view the list of audit policies.

Audit policies are managed on the Audit Policies page. Select Administration > Audit Management to display the Audit Management page, then click the Audit Policies link to display the Audit Policies page. Table 49, page 181 describes the information on the Audit Policies page.

Table 49. Audit Policies page information

<table>
<thead>
<tr>
<th>Column Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>The name of the audit policy.</td>
</tr>
<tr>
<td>Accessor Name</td>
<td>The name of the user, group, or role that are assigned this audit policy.</td>
</tr>
<tr>
<td>Is Group</td>
<td>Indicates whether the user specified in the Accessor Name column is belongs to a group.</td>
</tr>
</tbody>
</table>

Creating, modifying, or deleting an audit policy, page 182 provides information about creating or modifying an audit policy.
Creating, modifying, or deleting an audit policy

You must be the Install Owner to create, modify, or delete an audit policy.

To create, modify, or delete an audit policy:

1. Connect to the repository and navigate to Administration > Audit Management.
   The Audit Management page displays.
2. Click Audit Policies.
   The Audit Policies page displays.
3. Do one of the following:
   • To create an audit policy, click File > New > Audit Policy
     The New Audit Policy page displays. Enter the policy information as described in Table 50, page 182.
   • To modify an audit policy, select the audit policy, then select View > Properties > Info.
     The Audit Policy Properties page displays. Modify the policy information as described in Table 50, page 182.
   • To remove an audit policy, select the audit policy, then select File > Delete.
   • To save a copy of an audit policy, select the audit policy, then select File > Save As ....
4. Click OK to save your changes.

Table 50. Audit policy information

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>The name of the audit policy.</td>
</tr>
<tr>
<td>Accessor Name</td>
<td>The user, group, or role to which this audit policy is assigned.</td>
</tr>
<tr>
<td>Audit Policy Rules</td>
<td>Specifies the policy rules, as follows:</td>
</tr>
<tr>
<td></td>
<td>• Click Add to add a rule. The Create/Edit Rule page displays. Select an attribute and enter a value for the attribute.</td>
</tr>
<tr>
<td></td>
<td>• Select an attribute name, then click Edit to modify the rule. The Create/Edit Rule page displays. Modify the attribute.</td>
</tr>
<tr>
<td></td>
<td>• Select an attribute name, then click Remove to delete the rule.</td>
</tr>
<tr>
<td></td>
<td>There must be at least one rule or condition to save the audit policy.</td>
</tr>
</tbody>
</table>

Audit Policy example

The following audit policy example specifies the Test purge policy that enables user1 to purge the audit record for the object_type attribute type1 and the is_archived attribute T.
Table 51. Audit policy example values

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Test</td>
</tr>
<tr>
<td>Accessor Name</td>
<td>user1</td>
</tr>
</tbody>
</table>

Audit Policy Rules

<table>
<thead>
<tr>
<th>Attribute Name</th>
<th>Attribute Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>object_type</td>
<td>type1</td>
</tr>
<tr>
<td>is_archived</td>
<td>T</td>
</tr>
</tbody>
</table>

The policy described in this example only protects audit records that satisfy the policy. For example, the policy does not protect audit records that have the is_archived attribute set to F. Any user with purge audit extended privilege can delete those records.

Registering audits

The Register Audit page specifies the properties that are audited for an object or object instance.

Select the properties as described in Table 52, page 183 to define the audited properties and register the object or object instance for auditing.

The following fields are disabled:

- Application Code
- Lifecycle
- State
- Has signature manifested
- Include all subtypes
- Authentication Required

These fields are enabled only for auditing by object type.

Table 52. Object and object instance auditing properties

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Attributes</td>
<td>Records the values of particular properties of the object in the audit trail. Click <strong>Select Attributes</strong> to access the <strong>Choose an attribute</strong> page. Select the properties whose values you want to record, click &gt;, then click <strong>Add</strong>. To remove any properties, select them on the right-hand side of the page and click &lt;. Click <strong>OK</strong> when you are finished.</td>
</tr>
<tr>
<td>Add</td>
<td>Click to access the <strong>Choose an event</strong> page and select the events you want to register.</td>
</tr>
</tbody>
</table>
Adding, modifying, or removing audits

Register Audit page lists object instances or an object type that you selected for auditing, as well as the audited criteria and events. On this page, you can add, edit, or remove audits.

For object type:
- To add an audit, select the object name, then click Add Audit.
- To modify an audit, select the object, then click Edit.
- To remove an audit, select the object, then click Remove.

For object instance:
- To add or modify an audit, select the object, then click Edit.
  
  Note: The Add Audit button is disabled for object instance.

- To remove an audit, select the object, then click Remove.

Verifying or purging audit trails

Audit trails are displayed on the Audit Trails page after a search query has been issued, as described in Search audit, page 180.

On the Audit Trails page, you can
- View audit trail properties by selecting an audit trail, then selecting View > Info > Properties.
- Verify an audit record by right-clicking an audit trail and selecting Tools > Verify Audit Record.
  
  Only signed audit trails can be verified.
- Purge an audit record by right-clicking an audit trail and selecting Tools > Purge Audit Record(s).
  
  To purge more than one audit record, select the audit trails, then Tools > Purge Audit Record(s).
  
  You must have Purge Audit privileges to purge audit records. If the audit record is protected by an audit policy, you can only purge the record, if the purge policy is assigned to you or a group of which you are a member.
To navigate back to the Audit Management list page, click **Audit Management** at the top of the page.
Chapter 7

Job Management

This chapter contains the following topics:

- Jobs, page 187
- Methods, page 228
- Administration methods, page 235

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.

The *EMC Documentum Distributed Configuration Guide* provides more information on federation and replication jobs.
Job descriptions

These jobs are automatically created with each repository. The descriptions discuss arguments that can be modified for each job.

- ACL replication (dm_ACLReplication), page 189
- ACL replication (dm_ACLRepl_repository), page 189
- Archive (dm_DMArchive), page 192
- Audit management (dm_AuditMgt), page 189
- Consistency checker (dm_ConsistencyChecker), page 190
- Content replication (dm(ContentReplication), page 191
- Content warning (dm_ContentWarning), page 191
- Data dictionary publisher (dm_DataDictionaryPublisher), page 191
- Database space warning (dm_DBWarning), page 192
- Distributed operations (dm_DistOperations), page 192
- Dmclean (dm_DMClean), page 192
- Dmfilescan (dm_DMfilescan), page 193
- Federation copy (dm_FederationCopy), page 193
- Federation export (dm_FederationExport), page 193
- Federation import (dm_FederationImport), page 193
- Federation status (dm_FederationStatus), page 194
- Federation update (dm_FederationUpdate), page 194
- File report (dm_FileReport), page 194
- Group rename (dm_GroupRename and dm_GroupRename_Java), page 194
- LDAP synchronization (dm_LDAPSynchronization), page 195
- Log purge (dm_LogPurge), page 196
- Queue management (dm_QueueMgt), page 196
- Remove expired retention objects (dm_RemoveExpiredRetnObjects), page 197
- Rendition manager (dm_RenditionMgt), page 198
- SCS log purge (dm_SCSLogPurgeJob), page 198
- State of repository report (dm_StateOfDocbase), page 198
- Swap info (dm_SwapInfo), page 199
- Update statistics (dm_UpdateStats), page 199
- Usage tracking (dm_usageReport), page 199
- User change home repository (dm_UserChgHomeDb and dm_UserChgHomeDb_Java), page 200
- User rename (dm_UserRename and dm_UserRename_Java), page 200
• Version management (dm_VersionMgt), page 201
• WfmsTimer (dm_WfmsTimer), page 201

**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. The EMC Documentum Distributed Configuration Guide provides complete information on replication and replication jobs.

**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. The EMC Documentum Distributed Configuration Guide provides complete information on replication and replication jobs.

**Asynchronous Write (dm_AsynchronousWrite)**

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.

**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.

The following table describes the arguments for the dm_AuditMgt job that can be modified.
Table 53. dm_AuditMgt arguments

<table>
<thead>
<tr>
<th>Argument</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>window_interval</td>
<td>Defines window, in minutes, in which the job can run.</td>
</tr>
<tr>
<td>queueperson</td>
<td>Specifies the user who receives Inbox and email notifications from the job.</td>
</tr>
<tr>
<td>cutoff_days</td>
<td>Specifies the age of the objects to delete. The default value is 90 days.</td>
</tr>
<tr>
<td>custom_predicate</td>
<td>The custom Predicate argument is applied to those items meeting the age requirement specified in the cutoff_days argument. By default, the custom predicate includes three conditions:</td>
</tr>
<tr>
<td></td>
<td>• delete_flag=TRUE</td>
</tr>
<tr>
<td></td>
<td>This condition cannot be modified.</td>
</tr>
<tr>
<td></td>
<td>• dequeued_date=value (value is computed using the cutoff_days argument)</td>
</tr>
<tr>
<td></td>
<td>This condition cannot be modified.</td>
</tr>
<tr>
<td></td>
<td>• r_gen_source=1</td>
</tr>
<tr>
<td></td>
<td>Directs the server to delete only audit trail objects generated by system-defined events. To remove only audit trail objects generated by user-defined events, change the value to 0. To remove audit trail objects generated by both system- and user-defined events, remove the r_gen_source expression from the custom predicate.</td>
</tr>
<tr>
<td></td>
<td>You can also add other conditions (for example, event=approved) to the default custom predicate.</td>
</tr>
</tbody>
</table>

The Audit Management tool generates a status report that lists the deleted dm_audittrail entries. The report is saved in the /System/Sysadmin/Reports directory. The Audit Management tool is installed in the inactive state. The first time you execute the tool, it can 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 does not exist in the repository, and so forth. The consistency checker does not fix any of the inconsistencies. Contact Documentum Technical Support for assistance in correcting errors 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.
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_ContentReplicationservername.object_name

The jobs target_server property identifies the local server performing the replication using the format repository.servername@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.

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.
Database space warning (dm_DBWarning)

The Database Space Warning tool scans the RDBMS to determine how full the Oracle tablespace 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.

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.

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. The Archive tool is active by default and runs once daily.

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 the orphaned content objects. The Dmclean tool performs these operations and (optionally) runs the generated script.

When the agent exec program invokes the script, the tool generates a report showing which ACLs, notes, and workflow templates are removed. The report also shows the orphaned content objects that will be removed if the generated API script is executed. 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 orphaned 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. The EMC Documentum Distributed Configuration Guide provides complete information on repository federations and the federation jobs.

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. The EMC Documentum Distributed Configuration Guide provides complete information on repository federations and the federation jobs.

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. The EMC Documentum Distributed Configuration Guide provides complete information on repository federations and the federation jobs.
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. The EMC Documentum Distributed Configuration Guide provides complete information on repository federations and the federation jobs.

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. The EMC Documentum Distributed Configuration Guide provides complete information on repository federations and the federation jobs.

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.

Group rename (dm_GroupRename and dm_GroupRename_Java)

The group rename job renames repository groups and works in conjunction with the Groups pages in Documentum Administrator. By default, the job is installed in the inactive state.
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 dm_GroupRename method is available as a Docbasic or a Java method. The difference between the two method versions is that the Java version also supports international characters, including multibyte characters. By default, the group rename job points to the Docbasic version, dm_GroupRename. To use the Java version, you must change method name in the job properties to point to the dm_GroupRename_Java method.

To change the method name:

1. In Documentum Administrator select Job Management > Jobs.
   The Jobs page displays.
2. Select the dm_GroupRename job.
3. Right-click the job and select Properties.
   The Job Properties page displays.
4. Click the Method tab.
5. Click Select Method and select the dm_GroupRename_Java method in the Name column.
6. Click OK to save the changes.

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 Linux 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.

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>
<thead>
<tr>
<th>Log type</th>
<th>Delete from</th>
</tr>
</thead>
<tbody>
<tr>
<td>Server log files</td>
<td>Documentum Server installation log location</td>
</tr>
<tr>
<td>Connection broker log files</td>
<td>Documentum Server installation log location</td>
</tr>
<tr>
<td>Agent Exec log files</td>
<td>Documentum Server installation log location</td>
</tr>
<tr>
<td>Session log files</td>
<td>Documentum Server installation log location</td>
</tr>
<tr>
<td>Result log files</td>
<td>Temp cabinet</td>
</tr>
<tr>
<td>Job log files</td>
<td>Temp cabinet</td>
</tr>
<tr>
<td>Job reports</td>
<td>/System/Sysadmin/Reports folder</td>
</tr>
<tr>
<td>Lifecycle log files</td>
<td>Documentum Server installation log location</td>
</tr>
</tbody>
</table>

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. [SCS log purge (dm_SCSLogPurgeJob), page 198](#) provides 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-addressed 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. *Storage, page 285* provides more information on retention type storage areas.

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.  
Dmclean (dm_DMClean), page 192 provides more information on Dmclean.

Refer to CHECK RETENTION_EXPIRED in the Administration method operations section of the
EMC Documentum 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 Dmclean's 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.

**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 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. 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 SQL Server 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.

**Usage tracking (dm_usageReport)**

EMC provides a complimentary application, EMC Asset Management & Planning (AMP), that collates usage data from multiple global registries and can generate a variety of reports and documents about software usage. **EMC Documentum Asset Management & Planning (AMP) User Guide** contains information about obtaining, installing, and configuring AMP. **Appendix A, AMP and Usage Tracking** provides more details about this feature.

Content Server tracks software usage by recording login times. The Content Server global registry contains a registered table, dm_usage_log. This table contains a record of the first and the latest login time for each user of each application that connects to Content Server. A user, dm_report_user, was created when the global registry was configured. This user has read-only access to the dm_usage_log table. The initial password for dm_report_user is the global registry user password.
The `dm_usageReport` job runs monthly to generate a usage report. To view the report, refer to Viewing job reports, page 226. You can also generate a current report. To generate a current report, refer to Running jobs, page 225.

The information stored in `dm_usage_log` can also be exported from the global registry by using a utility program. Execute the following Java utility:

```
java com.documentum.server.impl.method.license.ExportUsageLog
repository dm_report_user password
```

Where `repository` is the global registry name and `password` is the `dm_report_user` password. Use your OS shell tools to redirect the output to a file.

**User change home repository (dm_UserChgHomeDb and dm_UserChgHomeDB_Java)**

The User Change Home Repository job changes a the home repository of a user.

The `dm_UserChgHomeDb` method is available as a Docbasic or a Java method. The difference between the two method versions is that the Java version also supports international characters, including multibyte characters. By default, the `rename` job points to the Docbasic version, `dm_UserChgHomeDb`. To use the Java version, you must change method name in the job properties to point to the `dm_UserChgHomeDb_Java` method.

**To change the method name:**

1. In Documentum Administrator select Job Management > Jobs.
   
   The Jobs page displays.
2. Select the `dm_UserChgHomeDb` job.
3. Right-click the job and select Properties.
   
   The Job Properties page displays.
4. Click the Method tab.
5. Click Select Method and select the `dm_UserChgHomeDb_Java` method in the Name column.
6. Click OK to save the changes.

The `dm_UserChgHomeDb` job works in conjunction with the user pages in Documentum Administrator. Changing the home repository of a user, page 146 provides more information about changing the home repository of user.

**User rename (dm_UserRename and dm_UserRename_Java)**

The User Rename job changes the user name for a particular user. By default, the User Rename job is installed in the inactive state.

The `dm_UserRename` method is available as a Docbasic or a Java method. The difference between the two method versions is that the Java version also supports international characters, including multibyte characters. By default, the User Rename job points to the Docbasic version,
dm_UserRename. To use the Java version, you must change method name in the job properties to point to the dm_UserRename_Java method.

To change the method name:
1. In Documentum Administrator select Job Management > Jobs.
   The Jobs page displays.
2. Select the dm_UserRename job.
3. Right-click the job and select Properties.
   The Job Properties page displays.
4. Click the Method tab.
5. Click Select Method and select the dm_UserRename_Java method in the Name column.
6. Click OK to save the changes.

Reassigning objects to another user, page 145 provides more information about changing a user name.

Version management (dm_VersionMgt)

The Version Management tool removes unwanted versions of documents from the repository. This tool automates the Destroy and Prune methods.

The EMC Documentum Content Server Fundamentals provides detail on the discussion of how Documentum versioning works.

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 192.

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.

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 hour by default.

Creating a job

Before you create a job, determine which method the job runs 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. Methods, page 228 provides information about creating method objects.

The New Job and Job Properties pages are identical for standard jobs, replication jobs, records migration jobs, remove expired retention objects, BOCS caching jobs, and job sequences. For instructions about creating a specific type of job, refer to:

- Creating replication jobs, page 208
- Creating records migration jobs, page 215
- Creating remove expired retention objects jobs, page 219
- Creating BOCS caching jobs, page 220
- Creating job sequences, page 222

**To create a basic 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 page with the Info tab selected.
3. Enter the general job information on the Info tab, as described in Table 55, page 202.
4. Click the Schedule tab and enter the job schedule information, as described in Table 56, page 204.
5. Click the Method tab and enter the job method information, as described in Table 57, page 206.
6. Click the SysObject Info tab and enter the job SysObject information, as described in Creating, viewing, or modifying SysObject properties, page 207.
7. Click Finish to save your changes.

**Table 55. Job Info properties**

<table>
<thead>
<tr>
<th>Field label</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>The name of the job object.</td>
</tr>
<tr>
<td>Job Type</td>
<td>A label identifying the job type.</td>
</tr>
<tr>
<td></td>
<td>If you are creating a replication job, records migration job, remove expired retention object, BOCS caching job, or a job sequence, this field is automatically populated with the associated job type.</td>
</tr>
<tr>
<td>Trace Level</td>
<td>Controls how much information is recorded in trace logs. May be set from 0 to 10. Viewing job trace logs, page 227 provides instructions on viewing trace logs.</td>
</tr>
<tr>
<td>Designated Server</td>
<td>When more than one server runs against a repository, use to designate a server to run the job. The default is Any Running Server.</td>
</tr>
</tbody>
</table>
### Field label | Description
--- | ---
State | Determines how the job runs:
• If set to Active, the job runs as scheduled.
• If set to Inactive, the job does not run automatically, but can be executed manually.
Job Start Date | Specifies when the job was started. This option is a read-only field that only displays for existing jobs.

### Options
- **Deactivate on Failure** | Specifies whether to make the job inactive if it does not run successfully.
- **Run After Update** | Specifies whether to run the job immediately after any changes to the job are saved.
- **Save If Invalid** | Specifies whether to save the job object if Documentum Administrator is unable to validate the job.

### Job Run History
- **Last Run** | Displays the last date and time the job ran and was completed. This option is a read-only field that displays for existing jobs.
- **Last Status** | Displays the last time the job completed and the length of time the job took to run. This option is a read-only field that displays for existing jobs.
- **Last Return Code** | Displays the last value returned by the job. This option is a read-only field that displays for existing jobs.
- **Runs Completed** | Displays the number of times the job has run to completion. This option is a read-only field that displays for existing jobs.

---

### Changing the schedule of a job

Use these instructions to modify a job schedule, whether the job is a standard job, replication job, remove expired retention objects 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.

5. Change the job schedule as described in Table 56, page 204.

6. Click OK.

**Table 56. Job Schedule properties**

<table>
<thead>
<tr>
<th>Field label</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Next Run Date and Time</td>
<td>Specifies the next start date and time for the job.</td>
</tr>
<tr>
<td></td>
<td>The default is the current date and time.</td>
</tr>
<tr>
<td>Repeat</td>
<td>Specifies the time interval in which the job is repeated.</td>
</tr>
<tr>
<td>Frequency</td>
<td>Specifies how many times the job is repeated.</td>
</tr>
<tr>
<td></td>
<td>For example, if Repeat is set to Weeks and Frequency is set to 1, the job repeats every week.</td>
</tr>
<tr>
<td></td>
<td>If Repeat is set to weeks and Frequency is set to 3, the job repeats every three weeks.</td>
</tr>
<tr>
<td>End Date and Time</td>
<td>Specifies the end date and time for the job.</td>
</tr>
<tr>
<td></td>
<td>The default end date is 10 years from the current date and time.</td>
</tr>
<tr>
<td>After</td>
<td>Specifies the number of invocations after which the job becomes inactive.</td>
</tr>
</tbody>
</table>

**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 Linux 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 Linux 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.

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. Click the Method tab on the the New Job or Job Properties page.
2. Enter the method information, as described in Table 57, page 206.
3. Click OK to save the changes.

Table 57. Job method properties

<table>
<thead>
<tr>
<th>Field label</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Method Name</td>
<td>Specifies the name of the method that is associated with the job.</td>
</tr>
<tr>
<td></td>
<td>Click Select Method to display the Choose a method page. Select a method</td>
</tr>
<tr>
<td></td>
<td>name and click OK.</td>
</tr>
<tr>
<td></td>
<td>Locating a method for a job, page 207 provides instructions to locate a</td>
</tr>
<tr>
<td></td>
<td>method.</td>
</tr>
<tr>
<td>Arguments</td>
<td>Specifies the method arguments.</td>
</tr>
<tr>
<td></td>
<td>Click Edit to display the Method Arguments page. Enter new arguments,</td>
</tr>
<tr>
<td></td>
<td>remove unnecessary arguments, or change the values to the method by the</td>
</tr>
<tr>
<td></td>
<td>job.</td>
</tr>
<tr>
<td></td>
<td>Many jobs take the queueperson and window_interval arguments.</td>
</tr>
<tr>
<td></td>
<td>• The queueperson argument defines which repository user receives the</td>
</tr>
<tr>
<td></td>
<td>inbox and email notifications generated by the jobs. If you do not</td>
</tr>
<tr>
<td></td>
<td>designate a repository user for a specific job, the notifications are</td>
</tr>
<tr>
<td></td>
<td>sent to the user identified by the operator_name property of the server's</td>
</tr>
<tr>
<td></td>
<td>server config object. This property is set to the repository owner's name</td>
</tr>
<tr>
<td></td>
<td>by default.</td>
</tr>
<tr>
<td></td>
<td>• The window_interval argument defines a window on either side of the job's</td>
</tr>
<tr>
<td></td>
<td>scheduled run time in which the job can run. This ensures that if a</td>
</tr>
<tr>
<td></td>
<td>server must be restarted, the startup is not delayed by jobs that must be</td>
</tr>
<tr>
<td></td>
<td>run.</td>
</tr>
<tr>
<td>Pass Standard Arguments</td>
<td>Select this option to pass the standard arguments for the method.</td>
</tr>
<tr>
<td></td>
<td>The standard arguments are:</td>
</tr>
<tr>
<td></td>
<td>• Repository owner</td>
</tr>
<tr>
<td></td>
<td>• Repository name</td>
</tr>
<tr>
<td></td>
<td>• Job ID</td>
</tr>
<tr>
<td></td>
<td>• Trace level</td>
</tr>
</tbody>
</table>
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 information (metadata) about an object. To see more or less information, click the show more or hide more links.

To create, view, or modify sysobject properties:
1. Access the SysObject Info page.
2. Type or modify the properties as described in Table 58, page 207.
3. Click OK to save your changes.

Table 58. SysObject properties

<table>
<thead>
<tr>
<th>Field label</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Title</td>
<td>A name or title for the object.</td>
</tr>
<tr>
<td>Subject</td>
<td>A subject that describes the object.</td>
</tr>
<tr>
<td>Keywords</td>
<td>One or more keywords that describe the object. Click Edit to add, modify, remove, or change the order of keywords.</td>
</tr>
<tr>
<td>Authors</td>
<td>One or more authors associated with the object. Click Edit to add, modify, remove, or change the order of authors.</td>
</tr>
<tr>
<td>Owner Name</td>
<td>The user who owns the object. Click Edit to add or modify the owner name.</td>
</tr>
<tr>
<td>Version Label</td>
<td>The version number of the object. Click Edit to add, modify, remove, or change the order of version numbers.</td>
</tr>
<tr>
<td>Checkout Date</td>
<td>The date on which the object was last checked out. This is a read-only property.</td>
</tr>
<tr>
<td>Checked Out By</td>
<td>The name of the user who checked out the object. This is a read-only property.</td>
</tr>
<tr>
<td>Field label</td>
<td>Description</td>
</tr>
<tr>
<td>--------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Created</td>
<td>The date on which the object was created. This is a read-only property.</td>
</tr>
<tr>
<td>Creator Name</td>
<td>The name of the user who created the object. This is a read-only property.</td>
</tr>
<tr>
<td>Modified</td>
<td>The date on which the object was last modified. This is a read-only property.</td>
</tr>
<tr>
<td>Modified By</td>
<td>The name of the user who modified the object. This is a read-only property.</td>
</tr>
<tr>
<td>Accessed</td>
<td>The date on which the object was last accessed. This is a read-only property.</td>
</tr>
</tbody>
</table>

**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. Creating job sequences, page 222 provides information on creating job sequences.

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. Choosing replication and security modes, page 213 provides complete information on choosing replication and security modes.

The Chapter 1, "Building Blocks and Models," in the EMC Documentum Distributed Configuration Guide provides more information about replication jobs.

**To create a replication job:**

1. Navigate to Administration > Job Management > Jobs.
   
   The Jobs list page displays.

   
   The New Replication Job page displays with the Info tab selected.

3. Enter general replication job information on the Info tab, as described in Table 55, page 202.
4. Click the **Schedule** tab and enter schedule information for the replication job, as described in Table 56, page 204.

5. Click the **From Source** tab and enter source repository information for the replication job, as described in Selecting the source repository for a replication job, page 209.

6. Click the **To Target** tab and enter target repository information for the replication job, as described in Selecting the target repository for a replication job, page 209.

7. Click the **Replication Options** tab and enter replication job options for the replication job, as described in Setting replication job options, page 210.

8. Click the **SysObject Info** tab and enter SysObject information for the replication job, as described in Creating, viewing, or modifying SysObject properties, page 207.

9. Click **Finish** to save your changes.

**Selecting the source repository for a replication job**

The From Source tab displays when you are creating or modifying a replication job and is used to select the source repository for the replication job. The source repository is the repository from which objects are replicated.

Creating replication jobs, page 208 provides instructions on how to access the New Replication Job - Source page and create new replication jobs.

**To select the source repository for a replication job:**

1. Type the login name of a superuser in the source repository.
2. Type the password for the superuser you chose in step 1.
3. On Windows, type the name of the domain where the source repository resides.
4. 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.
5. Click **Select Path** to access the Choose a folder page, then select the source cabinet or navigate to the correct folder in a cabinet.
6. 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 To Target tab displays when you are creating or modifying a replication job and is used to select the target repository for a replication job. The target repository is the repository to which objects are replicated.
Creating replication jobs, page 208 provides instructions on how to access the New Replication Job - To Target page and create new replication jobs.

**To select the target repository:**

1. Type the name and password of a superuser in the target repository.
2. On Windows, type the name of the domain where the target repository resides.
3. 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.
4. Click Select Path to access the Choose a folder page, then select the target cabinet or navigate to the correct folder in a cabinet, and click OK.
5. Optionally, click Select Owner to access the Choose a user page, then select the user who is the owner of the target repository, and click OK.
   This action updates objects to the owner you choose. Most replication jobs do not require this.
6. Click Select Permission Set to access the Choose a permission set page, then select a permission assigned to the replica objects, and click OK.
   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.
7. Click Select Storage to access the Choose a storage page, then select a storage area for the content associated with the replica, and click OK.
   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.
8. 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 Replication Options tab displays when you are creating or modifying a replication job pages are is used to set replication job options.

Creating replication jobs, page 208 provides instructions on how to create new replication jobs.

**To set replication options:**

1. Enter the replication options, as described in Table 59, page 211.
2. Click a tab to move to another Job Properties page, or click OK or Cancel to return to the Jobs list page.
### Table 59. Replication options

<table>
<thead>
<tr>
<th>Field label</th>
<th>Description</th>
</tr>
</thead>
</table>
| Code Page            | Specifies the correct code page for the replication job. Keep the value at the default, UTF-8, unless it must be changed.  
Select **Full Refresh** 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.  
Select **Fast Replication**, to use fast replication.  

**Caution:** Fast replication does not replicate all relationships. The *EMC Documentum Distributed Configuration Guide* provides the detailed information. |
| Full Text Indexing   | Specifies the full-text indexing mode. Valid options are:  
- **Use target repository settings for indexing:** The same documents are indexed in the source and target.  
- **Do not index replicas:** None of the replicas are marked for indexing.  
- **Index all replicas:** All replicas in a format that can be indexed are marked for indexing. |
| Replication Mode     | Specifies the replication mode.  
You can select federated mode whether or not the source and target repositories are in a federation. *Choosing replication and security modes, page 213* provides more information on selecting a replication mode.  
Nonfederated replication mode is called external replication mode in the *EMC Documentum Distributed Configuration Guide*. |
| Security Option      | Specifies 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.  
*Choosing replication and security modes, page 213* provides more information on choosing a security mode. |
### Field label | Description
--- | ---
Maximum objects per transfer | Specifies the maximum number of objects dumped and transferred in each operation. When selected, 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. Select **Manual Transfer** if you intend to manually move the dump file from the source to the target, then click **Select User** next to the **Transfer Operator** field.
Transfer operator | Specifies the user who manually transfers the replication job. 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.

---

### 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 permission set:**

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 Replication Options tab, you select a replication mode and a security mode.

The replication modes are:

- Federated mode, which can 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 *EMC Documentum Distributed Configuration Guide*. This mode can 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, as described in Table 60, page 214.

The sections External Replication Mode and Federated Replication Mode in Chapter 1, Building Blocks and Models, in the *EMC Documentum Distributed Configuration Guide* provides more information about the two replication modes.

**Table 60. Security mode behavior**

<table>
<thead>
<tr>
<th>Selection</th>
<th>Replication Mode</th>
</tr>
</thead>
</table>
| Federated and Preserve | • If the permission set of a replicated object exists in the target repository, the replica is assigned that permission set.  
                         • If the permission set of a replicated object does not exist in the target repository, the 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. |
| Non-Federated and Preserve | • If the permission set of a replicated object exists in the target repository, the replica is assigned that permission set.  
                         • If the permission set of a replicated object 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 Target tab. If no permission set is chosen, the server creates a default permission set that assigns RELATE permission to the every user 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. |
Creating records migration jobs

Records migration jobs move content files from one storage area to another. 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 displays.
   The New Records Migration Job page displays with the Info tab selected.
3. Enter information on the Info tab, as described in Table 55, page 202.
4. Click the Schedule tab and enter schedule information for the records migration job, as described in Table 56, page 204.
5. Click the Rules tab and enter rules information for the records migration job, as described in Setting the rules of a records migration job, page 216.
6. Click the SysObject Info tab and enter SysObject information for records migration job, as described in Creating, viewing, or modifying SysObject properties, page 207.
7. Click Finish.

Setting the rules of a records migration job

Use the Rules tab on 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.
Defining selection criteria for a records migration job, page 217 provides instructions about entering information on the Selection Criteria page.

- To select objects by query, select **By query**.
  
The drop-down beside the **By query** is enabled. Select the query object (data from dm_query type) from the drop-down list.

  The dm_query type is created by IAPI. For example:

  ```
  create,c, dm_query
  set,c, l, object_name
  myquery
  setfile,c,l, C:\mig_query.txt, crtext
  save,c, l
  ```

  The mig_query.txt file will have the actual query which will get set to dm_query object. The corresponding dm_query object needs to be used within records migration job.

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 218.

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 remove expired retention objects jobs**

This section contains information on how to create remove expired retention objects job.

**To create a remove expired retention objects job:**

1. Navigate to Administration > Job Management > Jobs.
   The Jobs list page displays.
2. Select File > New > Remove Retention Expired Objects.
   The New Remove Retention Expired Objects Job page displays with the Info tab selected.
3. Enter information on the Info tab, as described in Table 55, page 202.
4. Click the Schedule tab and enter schedule information for the remove retention expired objects job, as described in Table 56, page 204.
5. Click the Qualifier Rules tab and enter rules information for the remove retention expired objects job, as described in Setting the qualifier rules for the remove retention-expired objects job, page 204.
6. Click the SysObject Info tab and enter SysObject information for remove retention expired objects job, as described in Creating, viewing, or modifying SysObject properties, page 207.
7. Click Finish.

**Note:** The Remove expired retention objects (dm_RemoveExpiredRetnObjects), page 197 section contains information on the remove expired retention objects tool.
Creating BOCS caching jobs

A BOCS content caching job does the following:
• Creates and schedules a job to collect a set of documents based on a query.
• Creates caching requests for the documents with the BOCS destination information where the documents need to be.
• Sends caching requests to DMS on a predetermined schedule.

Any user type can create a BOCS caching job. 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 page displays with the Info tab selected.
3. Enter basic information for the BOCS caching job on the Info tab, as described in Table 55, page 202.
4. Click the Schedule tab and enter schedule information for the BOCS caching job, as described in Table 56, page 204.
5. Click the Caching Rules tab and enter caching information for the BOCS caching job, as described in Table 61, page 220.
6. Click the SysObject Info tab and enter Sysobject information for the BOCS caching job, as described in Creating, viewing, or modifying SysObject properties, page 207.
7. Click Finish to save your changes.

Setting BOCS caching rules

The caching rules specify the caching options and the content to be selected for caching to the BOCS servers.

Creating BOCS caching jobs, page 220 provides complete instructions on how to create a BOCS caching job.

Table 61. Caching rules properties

<table>
<thead>
<tr>
<th>Field label</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Object Type</td>
<td>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.</td>
</tr>
<tr>
<td>Field label</td>
<td>Description</td>
</tr>
<tr>
<td>----------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Selection Criteria</td>
<td>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.</td>
</tr>
<tr>
<td></td>
<td>• Select <strong>Build criteria (Maximum of 5 lines)</strong> to create up to five lines using query builder.</td>
</tr>
<tr>
<td></td>
<td>• Select <strong>DQL query</strong> to create more complex queries. There are no restrictions on the number of conditions in a DQL query. DQL queries for BOCS caching jobs are not validated by Documentum Administrator.</td>
</tr>
<tr>
<td>Network Location</td>
<td>The destination list of the cached content.</td>
</tr>
<tr>
<td></td>
<td>Click <strong>Select</strong> to access the Choose Network Locations page to select from which network locations the content should be cached.</td>
</tr>
<tr>
<td>Cutoff Date</td>
<td>Select a cutoff date preference.</td>
</tr>
<tr>
<td></td>
<td>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.</td>
</tr>
<tr>
<td></td>
<td>• Select <strong>Cache all selected content</strong> to cache all documents without considering the last modified date of the document.</td>
</tr>
<tr>
<td></td>
<td>• Select <strong>Cache only selected content added/modified after</strong> and then select a date, hour, minute, and second to cache documents based on the selected date and time criteria.</td>
</tr>
<tr>
<td>Expiration</td>
<td>Enter an expiration date at which the caching request will expire if it is not fulfilled by that date.</td>
</tr>
<tr>
<td>Previous</td>
<td>Click to move to the previous page.</td>
</tr>
<tr>
<td>Next</td>
<td>Click to move to the next page.</td>
</tr>
<tr>
<td>OK or Finish</td>
<td>Click to save the changes and return to the Jobs list page.</td>
</tr>
<tr>
<td>Cancel</td>
<td>Click to return to the Jobs list page without saving any changes.</td>
</tr>
</tbody>
</table>
Creating job sequences

A job sequence is a job that runs a series of other jobs. 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.

The following restrictions apply to job sequences:

- You must be a superuser to create a job sequence.
- 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 there is no 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.

To create a job sequence:

1. In Documentum Administrator, navigate to Administration > Job Management > Jobs.
   The system displays the Jobs list page.
2. Select File > New > Job Sequence.
   The New Job Sequence page displays with the Info tab selected.
3. Enter the general job information on the Info tab, as described in Table 55, page 202.
4. Click the Schedule tab and enter the job schedule information, as described in Table 56, page 204.
5. Click the Connection Info tab and enter the repository and job sequence information, as described in Table 62, page 223.
6. Click the SysObject Info tab and enter the job SysObject information, as described in Creating, viewing, or modifying SysObject properties, page 207.
7. Click Finish.
   The job is saved and the Jobs list page appears.
Providing repository and job information for a job sequence

Use the Connection Info tab on the New Job Sequence or Job Properties page to select repositories and to designate the jobs to run in a job sequence.

To provide connection and job information for a job sequence:

1. Click the Connection Info tab and enter information in the Job Repositories and Job Sequence Information section, as described in Table 62, page 223.
2. Click Finish.

Table 62. Job Connection Info properties

<table>
<thead>
<tr>
<th>Field label</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Add</td>
<td>Click <strong>Add</strong> to access the Choose Repositories page. The system displays a list of available repositories. Select the repositories in which you want to run jobs, click <strong>Add</strong>, then click <strong>OK</strong>. If a repository where you want to run a job is not listed, add a connection broker to which that repository projects. <a href="#">Creating or modifying connection broker projections, page 75</a> provides more information about adding a connection broker.</td>
</tr>
<tr>
<td>Remove</td>
<td>To remove a repository from the list, select the repository and click <strong>Remove</strong>. If jobs in the repository are part of the sequence, you must remove the jobs first.</td>
</tr>
<tr>
<td>Repository</td>
<td>The name of the repository where you want to run the job. 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.</td>
</tr>
<tr>
<td>User Name</td>
<td>The login name for the repository.</td>
</tr>
<tr>
<td>Password</td>
<td>The password for the repository.</td>
</tr>
<tr>
<td>Domain</td>
<td>Specify the domain for any repository running in domain-required mode.</td>
</tr>
</tbody>
</table>

Job Sequence Information
<table>
<thead>
<tr>
<th>Field label</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Add</td>
<td>Click <strong>Add</strong> to add jobs to the sequence. The system validates the connection information entered in the Job Repositories. 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 <strong>Add</strong>, then <strong>OK</strong>. 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.</td>
</tr>
<tr>
<td>Job Name</td>
<td>The name of the job that are in the job sequence.</td>
</tr>
<tr>
<td>Job Dependencies</td>
<td>Specifies the dependencies the job has on other jobs. Click <strong>Edit</strong> to designate the job dependencies for each job that must run after another job completes. Select the listed job(s) that must run before the current job runs, then click <strong>OK</strong>. 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. To remove a dependency, click <strong>Edit</strong> in the Job Sequence section to access the Choose jobs dependency page, clear the checkbox for any selected job, then click <strong>OK</strong>.</td>
</tr>
<tr>
<td>Repository</td>
<td>The name of the repository where the job sequence is run.</td>
</tr>
</tbody>
</table>

**Selecting jobs for a job sequence**

Use the instructions in this section to select jobs for the job sequence.

To access the Choose jobs page, click **Add** in the Job Sequence Information section on the Connection Info tab of the New Job Sequence or Job Properties page.

**To select jobs for a job sequence:**

1. 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**.
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 Connection Info tab of the New Job Sequence or Job Properties 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. Select the listed job(s) that must run before the current job runs.
2. To remove a dependency, click the row to clear the selection for any 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 203 provides 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). Setting the trace level for a job, page 226 provides information on setting a different trace level.

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.

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 that fail

Use the instructions in this section to configure a job so that it becomes inactive if it fails.

To deactivate jobs that fail:
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 Info tab of the Job Properties page.
3. Select the Deactivate on failure checkbox.
4. Click OK.

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. Jobs, page 187 provides information about creating jobs.

The executable invoked by the method can be stored in the file system or as content of the method object. If the method is executed by the Java method server, the entire custom or xml app jar must be stored in the $DOCUMENTUM_SHARED\<bob\>\server\DctmServer_MethodServer\deploy\ServerApps.ear\DmMethods.war\WEB-INF\lib directory. For workflow methods, the .jar files must be placed under the Process Engine deployment in the $DOCUMENTUM_SHARED<bob>/server/DctmServer_MethodServer/deploy/bpm.ear/bpm.war/WEB-INF/lib directory.

By default, all repositories contain methods used by Content Server. All methods with object names that begin with dm_ are default methods.

Creating or modifying methods

The executable invoked by the method can be stored in an external file or as content of the method object. All other programs, except Java programs, are stored on the Content Server file system or in the repository as the content of the method object.

If the program is a Java method and you want to execute it using the Java method server, install the method on host file system of the application server. Only the application server instance installed during Content Server installation can execute Java methods. Do not store the program in the repository as the content of the method object.

Creating methods requires superuser privileges.

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 Methods list page displays.
2. Do one of the following:
   • To create a new method, select File > New > Method.
The Info tab on the New Method page displays. You must have superuser privileges to create a method.

- To modify a method, select the method and then select View > Properties > Info.
  The Info tab on the Method Properties page displays.
- To edit the method content, refer to Editing method content, page 234.

3. Enter or modify the method information as described in Table 63, page 229 and the optional Table 64, page 231.

4. Click OK to save your changes.
If you want to store the program as the content of the method object, you must import the content after the method is created, as described in Importing method content, page 231.

Table 63. Method Info tab properties

<table>
<thead>
<tr>
<th>Field label</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>The method name.</td>
</tr>
<tr>
<td>Verb</td>
<td>The method verb, including arguments.</td>
</tr>
<tr>
<td>Method Type</td>
<td>Specifies the programming language of the method. Valid values are:</td>
</tr>
<tr>
<td></td>
<td>• <strong>dmbasic</strong>: The method is written in Docbasic.</td>
</tr>
<tr>
<td></td>
<td>• <strong>dmawk</strong>: The method is written in dmawk.</td>
</tr>
<tr>
<td></td>
<td>• <strong>java</strong>: The method is written is Java and executed on the Java Method Server.</td>
</tr>
<tr>
<td></td>
<td>• <strong>program</strong>: The method is writing in a programming language, such as C or C++.</td>
</tr>
</tbody>
</table>

If the method is executed using Content Server or the dmbasic method server, and the executable is stored as content for the method, setting the method type to dmawk or dmbasic, directs the server to add -f in front of the filename. The server passs
<table>
<thead>
<tr>
<th>Field label</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Arguments</td>
<td>Specifies method arguments. Click <strong>Edit</strong> to add arguments.</td>
</tr>
<tr>
<td>Method Success Codes</td>
<td>Specifies method success codes. Click <strong>Edit</strong> to add success codes.</td>
</tr>
<tr>
<td>Method Success Status</td>
<td>Specifies the valid value for current status in the completed job. If this option is selected, the current status property value of the job must match the success status value after the job completes. The property is ignored if the option is not selected.</td>
</tr>
<tr>
<td>Timeout Minimum</td>
<td>The minimum timeout that can be specified on the command line for this procedure. The minimum timeout value cannot be greater than the default value specified in the timeout default field.</td>
</tr>
<tr>
<td>Timeout Default</td>
<td>The default timeout value for the procedure. The system uses the default timeout value if no other time-out is specified on the command line.</td>
</tr>
<tr>
<td></td>
<td>The default timeout value is 60 seconds and cannot be greater than the value specified in the timeout maximum field.</td>
</tr>
<tr>
<td>Timeout Maximum</td>
<td>The maximum timeout that can be specified on the command line for this procedure. The default is 300 seconds.</td>
</tr>
<tr>
<td>Launch Direct</td>
<td>Specifies whether the program is executed by the system call or exec API call. When the launch direct option is selected, the server uses the exec call to execute the procedure. In this case, the method verb must be a fully qualified path name.</td>
</tr>
<tr>
<td>Launch Asynchronously</td>
<td>Specifies whether the server runs the method asynchronously or not.</td>
</tr>
<tr>
<td></td>
<td>If this option is selected and the method is launched on the application server, setting SAVE_RESPONSE on to TRUE on the command line is ignored.</td>
</tr>
<tr>
<td></td>
<td>If this option is select and the method is launched on the method server or Content Server and SAVE_RESULTS is set to TRUE on the command line, the method is always launched synchronously.</td>
</tr>
<tr>
<td>Run As Owner</td>
<td>Specifies whether to run method to run as the installation owner account, with the privileges of the installation owner. If this option is not selected, the method runs with the privileges of the method user.</td>
</tr>
<tr>
<td></td>
<td>This option must be selected to execute a method on the method server or application server.</td>
</tr>
<tr>
<td>Trace Launch</td>
<td>Specifies whether to save internal trace messages generated by the method to the session log.</td>
</tr>
<tr>
<td>Use Method Server</td>
<td>Specifies whether to use the dmbasic method server or Java method server to execute a dmbasic or Java method.</td>
</tr>
</tbody>
</table>
Table 64. SysObject Info tab properties

<table>
<thead>
<tr>
<th>Field label</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Title</td>
<td>A descriptive title for the method.</td>
</tr>
<tr>
<td>Subject</td>
<td>A subject associated with the method.</td>
</tr>
<tr>
<td>Keywords</td>
<td>One or more keywords that describe the method. Click <strong>Edit</strong> to add keywords.</td>
</tr>
<tr>
<td>Authors</td>
<td>One or more method authors. Click <strong>Edit</strong> to add authors.</td>
</tr>
<tr>
<td>Owner Name</td>
<td>The name of the method owner. Click <strong>Edit</strong> to select a different owner.</td>
</tr>
<tr>
<td>Version Label</td>
<td>The current version label of the method. Click <strong>Edit</strong> to change the version label.</td>
</tr>
<tr>
<td>Checkout Date</td>
<td>The date when the method was checked out last.</td>
</tr>
<tr>
<td>Checked Out by</td>
<td>The name of the user who checked out the method.</td>
</tr>
<tr>
<td>Created</td>
<td>The date and time when the method was created.</td>
</tr>
<tr>
<td>Creator Name</td>
<td>The name of the user who created the method.</td>
</tr>
<tr>
<td>Modified</td>
<td>The date and time when the method was last modified.</td>
</tr>
<tr>
<td>Modified By</td>
<td>The name of the user who last modified the method.</td>
</tr>
<tr>
<td>Accessed</td>
<td>The time and date when the method was last accessed.</td>
</tr>
</tbody>
</table>

**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 228 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.

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 236
- Running administration methods, page 236

There are links to instructions for running all administrations methods in Running administration methods, page 236. 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 method arguments, 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 237
- CLEAN_LINKS, page 238
- DELETE_REPLICA, page 238
- DESTROY_CONTENT, page 239
- EXPORT_TICKET_KEY, page 240
- GET_PATH, page 240
- IMPORT_REPLICA, page 241
- IMPORT_TICKET_KEY, page 242
- MIGRATE_CONTENT, page 242
- PURGE_CONTENT, page 247
- REPLICATE, page 248
- RESTORE_CONTENT, page 249
- SET_STORAGE_STATE, page 250

The following sections provide more information about database methods:
- DB_STATS, page 251
- DROP_INDEX, page 251
- EXEC_SQL, page 252
• FINISH_INDEX_MOVES, page 252
• GENERATE_PARTITION_SCHEME_SQL, page 253
• MAKE_INDEX, page 255
• MOVE_INDEX, page 256
The following sections provide more information about full-text indexing methods.
• ESTIMATE_SEARCH, page 256
• MARK_FOR_RETRY, page 257
• MODIFY_TRACE, page 258
The following sections provide more information about trace methods:
• GET_LAST_SQL, page 258
• MODIFY_TRACE, page 258
• LIST_RESOURCES, page 259
• LIST_TARGETS, page 260
• SET_OPTIONS, page 261
The following section provides more information about the workflow method:
• RECOVER_AUTO_TASKS, page 262
• WORKFLOW_AGENT_MANAGEMENT, page 263

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.
h. 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 system administrator 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. Click **Run**.
   The results are displayed.

5. Click **Close**.
The system displays the Administration Methods page.

**EXPORT_TICKET_KEY**

The EXPORT_TICKET_KEY administration method encrypts and exports a login ticket from the repository to a client machine.

**To run the EXPORT_TICKET_KEY administration method:**

1. Navigate to Administration > Job Management > Administration Methods.
   The Administration Methods list page displays.
2. Click EXPORT_TICKET_KEY.
   The Parameters page displays.
3. Depending on the type of encryption software you are using, type an encryption key or password in the **Encrypt key** field.
   The server uses the encryption key or password to encrypt the login ticket before exporting it. The same encryption key is required for decrypting when the login ticket is imported.
4. Click **Run**.
   A dialog displays, prompting you to save the login ticket file.
5. Save the login ticket file to any desired location.
   The system runs the method and displays the Results page informing you that the login ticket was exported successfully.

**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 system administrator 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.

**IMPORT_TICKET_KEY**

The IMPORT_TICKET_KEY administration method decrypts a login ticket from a client machine and imports the ticket into the repository.

**To run the IMPORT_TICKET_KEY administration method:**

1. Navigate to **Administration > Job Management > Administration Methods**.
The Administration Methods list page displays.

2. Click **IMPORT_TICKET_KEY**.
The Parameters page displays.

3. Type the decryption key in the **Decrypt key** field.
The decryption key is used to decrypt the login ticket before it is imported into the repository. You must provide the same key that was used to encrypt the login ticket.

4. Type the path to the login ticket in the **Ticket location** field or browse for the ticket location.

5. Click **Run**.
The system runs the method and displays the Result page. The Results page displays an error message if the login ticket is corrupted, the decryption key is invalid, the login ticket is invalid, the login ticket file does not exist, or if the login ticket times out.

6. Restart the Content Server after successfully importing the login ticket to make your changes take effect.

**MIGRATE_CONTENT**

The MIGRATE_CONTENT administration method migrates content files from one storage area to another.
The MIGRATE_CONTENT method requires superuser privileges to migrate:
• Single content objects.
• Single sysobjects.
• Sets of content objects qualified by a DQL predicate against dmr_content.
• 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, read-only, or WORM (Write Once Read Many).

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.
• 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.

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.

To migrate a single object:
1. Navigate to Administration > Job Management > Administration Methods. The system displays the Administration Methods list page.
2. Click MIGRATE_CONTENT. The system displays the Parameters page.
3. Specify the parameters for moving the single object, as described in Table 65, page 243.
4. Click Run.

Table 65. Parameters for moving a single object

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Migrate</td>
<td>Select A single object from the drop-down list.</td>
</tr>
</tbody>
</table>
### Description

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Content</td>
<td>Click <strong>Select Object</strong>, then select an object type from the <strong>Select From</strong> drop-down list. Specify a limiting Where clause, or leave the <strong>Where</strong> field blank to select all objects in the repository. To display all object versions, select the <strong>Use all versions</strong> checkbox and then click <strong>Go</strong>. Select the objects to migrate and click <strong>Add</strong>. Select <strong>Remove the original source</strong> to remove the original content file. The <strong>Remove the original source</strong> option cannot be edited, if the selected object belongs to an external store.</td>
</tr>
<tr>
<td>Path</td>
<td>Click <strong>Select Path</strong> and select a location on the server file system for the log file path.</td>
</tr>
<tr>
<td>Target</td>
<td>Select a target file store from the drop-down list.</td>
</tr>
<tr>
<td>Source Direct Access</td>
<td>Specifies whether the content files in the source store can be directly accessed through a full file path. This option is only available if the <strong>Source</strong> is an external store and the <strong>Target</strong> is either a file store or a ca store.</td>
</tr>
<tr>
<td>Migrate With</td>
<td>Specifies whether the source content is copied or moved to the target store during migration. Direct Move is applicable to file stores only. This option is only available if the <strong>Source</strong> is an external store and the <strong>Target</strong> is either a file store or a ca store.</td>
</tr>
<tr>
<td>Update Only</td>
<td>This option is used only in conjunction with the Direct Copy or Direct Move option. When selected, move or copy commands are written to the log file specified in the <strong>Command File Name</strong> field. This option is only available if the <strong>Source</strong> is an external store and the <strong>Target</strong> is either a file store or a ca store.</td>
</tr>
<tr>
<td>Command File Name</td>
<td>A string that specifies a file path to a log file. This option is only available if the <strong>Source</strong> is an external store and the <strong>Target</strong> is either a file store or a ca store and if the <strong>Update Only</strong> option is selected.</td>
</tr>
</tbody>
</table>

**To migrate all content files in a file store:**

1. Navigate to Administration > Job Management > Administration Methods. The system displays the Administration Methods list page.
2. Click MIGRATE_CONTENT. The system displays the Parameters page.
3. Specify the parameters for moving the content, as described in Table 66, page 245.
4. Click Run.
Table 66. Parameters for moving all content in a store

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Migrate</td>
<td>Select <strong>All content in a filestore</strong> from the drop-down list.</td>
</tr>
<tr>
<td>Source</td>
<td>Select a source file store from the <strong>Source</strong> drop-down list. Select <strong>Remove the original source</strong> to remove the original content file. The <strong>Remove the original source</strong> option cannot be edited, if the selected object belongs to an external store.</td>
</tr>
<tr>
<td>Path</td>
<td>Click <strong>Select Path</strong> and select a location on the server file system for the log file path.</td>
</tr>
<tr>
<td>Target</td>
<td>Select a target file store from the drop-down list.</td>
</tr>
<tr>
<td>Maximum</td>
<td>Specifies the maximum number of objects to migrate. The default is to migrate all objects.</td>
</tr>
<tr>
<td>Batch Size</td>
<td>Specifies the number of objects migrated in a single transaction. The default value is 500. Multiple transactions are run until the maximum number of objects to migrate is reached.</td>
</tr>
<tr>
<td>Content Migration Threads</td>
<td>Specifies the number of internal sessions used to execute the method. The default value is 0, indicating that the migration executes sequentially. The value cannot exceed the Maximum Content Migration Threads value in the server configuration object.</td>
</tr>
<tr>
<td>Source Direct Access</td>
<td>Specifies whether the content files in the source store can be directly accessed through a full file path. This option is only available if the <strong>Source</strong> is an external store and the <strong>Target</strong> is either a file store or a ca store.</td>
</tr>
<tr>
<td>Migrate With</td>
<td>Specifies whether the source content is copied or moved to the target store during migration. Direct Move is applicable to file stores only. This option is only available if the <strong>Source</strong> is an external store and the <strong>Target</strong> is either a file store or a ca store.</td>
</tr>
</tbody>
</table>
To migrate objects selected by a query:

1. Navigate to Administration > Job Management > Administration Methods.
   The system displays the Administration Methods list page.

2. Click MIGRATE_CONTENT.
   The system displays the Parameters page.

3. Specify the parameters for moving the content, as described in Table 67, page 246.

4. Click Run.

Table 67. Parameters for moving content selected by a query

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Migrate</td>
<td>Select All content satisfying a query from the drop-down list.</td>
</tr>
<tr>
<td>Select Object Type to Migrate</td>
<td>Specify the object type to migrate.</td>
</tr>
<tr>
<td>Select r_object_id from dmr_content where</td>
<td>If you select dm_sysobject or its subtype, click Select to access the Choose a type page to select a subtype of dm_sysobject.</td>
</tr>
<tr>
<td>Path</td>
<td>Click Select Path and select a location on the server file system for the log file path.</td>
</tr>
<tr>
<td>Target</td>
<td>Select a target file store from the drop-down list.</td>
</tr>
<tr>
<td>Maximum</td>
<td>Specifies the maximum number of objects to migrate.</td>
</tr>
<tr>
<td>Batch Size</td>
<td>Specifies the number of objects migrated in a single transaction.</td>
</tr>
</tbody>
</table>

The default value is 500. Multiple transactions are run until the maximum number of objects to migrate is reached.
<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Content Migration Threads</td>
<td>Specifies the number of internal sessions used to execute the method.</td>
</tr>
<tr>
<td></td>
<td>The default value is 0, indicating that the migration executes sequentially. The value cannot exceed the Maximum Content Migration Threads value in the server configuration object.</td>
</tr>
<tr>
<td></td>
<td>This option is only available if a Content Storage Services license is enabled on the Content Server.</td>
</tr>
<tr>
<td>Source Direct Access</td>
<td>Specifies whether the content files in the source store can be directly accessed through a full file path.</td>
</tr>
<tr>
<td></td>
<td>This option is only available if the Source is an external store and the Target is either a file store or a ca store.</td>
</tr>
<tr>
<td>Migrate With</td>
<td>Specifies whether the source content is copied or moved to the target store during migration. Direct Move is applicable to file stores only.</td>
</tr>
<tr>
<td></td>
<td>This option is only available if the Source is an external store and the Target is either a file store or a ca store.</td>
</tr>
<tr>
<td>Update Only</td>
<td>This option is used only in conjunction with the Direct Copy or Direct Move option. When selected, move or copy commands are written to the log file specified in the Command File Name field.</td>
</tr>
<tr>
<td></td>
<td>This option is only available if the Source is an external store and the Target is either a file store or a ca store.</td>
</tr>
<tr>
<td>Command File Name</td>
<td>A string that specifies a file path to a log file.</td>
</tr>
<tr>
<td></td>
<td>This option is only available if the Source is an external store and the Target is either a file store or a ca store and if the Update Only option is selected.</td>
</tr>
</tbody>
</table>

If the MIGRATE_CONTENT method fails with an error, the entire batch transaction is rolled back. If the destination has content files that were created from the successful migrations within the batch, you can clean up those files running the Dmfilescan job, as described in Dmfilescan (dm_DMfilescan), page 193.

**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 system administrator 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.

The REPLICATE method returns TRUE if the operation succeeds or FALSE if it fails.

You must have system administrator 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 system administrator 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 system administrator 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, read-only, or WORM (Write Once Read Many).

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.

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.
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.

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.
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.

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, as described in Table 68, page 253.

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.

**Table 68. GENERATE_PARTITION_SCHEME_SQL parameters**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Operation</td>
<td>Select an operation from the dropdown list box to define the subcommand. The options are:</td>
</tr>
<tr>
<td></td>
<td>• <strong>DB_PARTITION</strong>: Generates a script to upgrade or convert a repository to a 6.5 partitioned repository. If selected:</td>
</tr>
<tr>
<td></td>
<td>— Select Partition Type or Table Name.</td>
</tr>
<tr>
<td></td>
<td>— If Table Name is defined, optionally define the Owner Name.</td>
</tr>
<tr>
<td></td>
<td>— Include object type is optional. Select to apply the partition operation to the dmi_object_type table.</td>
</tr>
<tr>
<td>Parameter</td>
<td>Description</td>
</tr>
<tr>
<td>----------------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td></td>
<td>— Last Partition and Last Tablespace are optional.</td>
</tr>
<tr>
<td></td>
<td>— In the Partitions section, Partition Name, Range, and Tablespace are required.</td>
</tr>
<tr>
<td><strong>ADD_PARTITION</strong></td>
<td>Generates a script to add a partition to a partitioned type. If selected:</td>
</tr>
<tr>
<td></td>
<td>— Select Partition Type or Table Name.</td>
</tr>
<tr>
<td></td>
<td>— If Table Name is defined, optionally define the Owner Name.</td>
</tr>
<tr>
<td></td>
<td>— Include object type is optional. Select to apply the partition operation to the dmi_object_type table.</td>
</tr>
<tr>
<td></td>
<td>— In the Partitions section, Partition Name, Range, and Tablespace are required.</td>
</tr>
<tr>
<td><strong>EXCHANGE_PARTITION</strong></td>
<td>Generates a script for bulk ingestion by loading data from an intermediate table into a new partition of a partitioned table. If selected:</td>
</tr>
<tr>
<td></td>
<td>— Partition Type and Table Name are mutually exclusive.</td>
</tr>
<tr>
<td></td>
<td>— If Table Name is defined, optionally define the Owner Name.</td>
</tr>
<tr>
<td></td>
<td>— Include object type is optional. Select to apply the partition operation to the dmi_object_type table.</td>
</tr>
<tr>
<td></td>
<td>— Partition Name, Range, and Tablespace are required.</td>
</tr>
<tr>
<td></td>
<td>— Temp Table Suffix is optional.</td>
</tr>
</tbody>
</table>

**Partition Type**
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.

**Table Name**
Type a table name. If you select Table Name, then you cannot select Partition Type.

**Include object type**
Optionally, select to apply the partition operation to the dmi_object_type table.

**Owner Name**
Type an owner name. This field is enabled only if Table Name is selected.

**Last Partition**
Optionally, type a name for the last partition. This field appears only when DB_PARTITION is selected as the operation.

**Last Tablespace**
Optionally, type a tablespace name for the last partition. This field appears only when DB_PARTITION is selected as the operation.
### 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.

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.

**MOVE_INDEX**

The MOVE_INDEX administration method moves an existing object type index from one tablespace or segment to another.

The MOVE_INDEX method returns TRUE if the operation succeeds or FALSE if it fails.

You must have system administrator 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.

**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. The ESTIMATE_SEARCH administration method is not available, if the connected repository is configured with the xPlore search engine.

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). Refer to the section in the EMC Documentum DQL Reference Manual on MARK_FOR_RETRY.

The MARK_FOR_RETRY method returns TRUE if the operation succeeds or FALSE if it fails.

You must have system administrator 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 system administrator 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 system administrator 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.

Issuing LIST_RESOURCES with RESET=T reinitializes heap_size_new to zero.

**root_heap_size_in_use**

How much, in bytes, of the main server threads heap is in use.

**root_heap_size_new**

A count of the bytes that the heap has grown or shrunk since the last LIST_RESOURCES call.

**max_processes**

The maximum number of processes that can be created by the account under which the server is running.

**server_init_file**

The full path to the servers server.ini file.

**initial_working_directory**

The full path to the directory containing the server executable.

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:

<table>
<thead>
<tr>
<th>Option</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>clean</td>
<td>Removes the files from the server common area.</td>
</tr>
<tr>
<td>crypto_trace</td>
<td>Cryptography and remote key management information.</td>
</tr>
<tr>
<td>debug</td>
<td>Traces session shutdown, change check, launch and fork information.</td>
</tr>
<tr>
<td>docbroker_trace</td>
<td>Traces connection broker information.</td>
</tr>
<tr>
<td>i18n_trace</td>
<td>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.</td>
</tr>
<tr>
<td>last_sql_trace</td>
<td>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. 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.</td>
</tr>
<tr>
<td>lock_trace</td>
<td>Traces Windows locking information.</td>
</tr>
<tr>
<td>net_ip_addr</td>
<td>Traces the IP addresses of client and server for authentication.</td>
</tr>
<tr>
<td>nettrace</td>
<td>Turns on RPC tracing. Traces Netwise calls, SSL, connection ID, client host address, and client hostname.</td>
</tr>
<tr>
<td>Option</td>
<td>Action</td>
</tr>
<tr>
<td>-----------------------</td>
<td>-------------------------------------------------------------------------</td>
</tr>
<tr>
<td>sql_trace</td>
<td>SQL commands sent to the underlying RDBMS for subsequent sessions, including the repository session ID and the database connection ID for each SQL statement.</td>
</tr>
<tr>
<td>trace_authentication</td>
<td>Traces detailed authentication information.</td>
</tr>
<tr>
<td>trace_complete_launch</td>
<td>Traces Linux process launch information.</td>
</tr>
<tr>
<td>trace_method_server</td>
<td>Traces the operations of the method server.</td>
</tr>
</tbody>
</table>

The SET_OPTIONS method returns TRUE if the operation succeeds or FALSE if it fails.

You must have system administrator 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.

### RECOVER_AUTO_TASKS

Run the RECOVER_AUTO_TASKS administration method to recover workflow tasks that have been claimed, but not yet processed by a workflow agent associated with a failed Content Server.

If a Content Server fails, its workflow agent is also stopped. When the server is restarted, the workflow agent recognizes and processes any work items it had claimed but not processed before the failure. However, if you cannot restart the Content Server that failed, you must recover those work items already claimed by its associated workflow agent so that another workflow agent can process them. The RECOVER_AUTO_TASKS administration method performs that recovery.

To run the RECOVER_AUTO_TASKS administration method:

1. Navigate to Administration > Job Management > Administration Methods.
   The system displays the Administration Methods list page.
2. Click RECOVER_AUTO_TASKS.
   The system displays the Parameters page.
3. Select a server from the Server Config drop-down list box.
   **Note:** Before executing the RECOVER_AUTO_TASKS administration method, make sure that the specified Content Server is not running.

4. Click Run.
   The system runs the method and then displays the results on the Result page.

5. Click Close.
   The system displays the Administration Methods list page.

---

**WORKFLOW_AGENT_MANAGEMENT**

Run the WORKFLOW_AGENT_MANAGEMENT method to start and shutdown a workflow agent.

**To run the WORKFLOW_AGENT_MANAGEMENT administration method:**

1. In Documentum Administrator, navigate to Administration > Job Management > Administration Methods.
   The system displays the Administration Methods list page.

2. Click WORKFLOW_AGENT_MANAGEMENT.
   The system displays the Parameters page.

3. Select a server from the Server Config drop-down list box.
   The first server in the drop-down list is selected by default. Content Server checks the status of the workflow agent corresponding to the selected server.

4. Do one of the following:
   - Click Start to start a workflow agent that is currently stopped.
     The Administration Method Results page displays a message and the current status of the workflow agent as Starting to indicate that the workflow agent startup is in progress. During the startup process the workflow agent cannot be stopped.
   - Click Shutdown to stop a workflow agent that is currently running.
     The Administration Method Results page displays a message and the current status of the workflow agent as Stopped.

     You have the option to provide a value in the Timeout field:
     - An integer value greater than 0: Content Server waits for the specified time for the workflow agent to shut down gracefully. If the time is exceeded, Content Server shuts down the workflow agent.
     - 0: Content Server shuts down the workflow agent immediately.

     If you do not provide a timeout value, Content Server uses the timeout value specified in the System Shutdown Timeout property of the server config object.

5. Click Close.
If the workflow agent startup or shutdown process fails, the Administration Method Results page displays an error message indicating the process failure and provides additional information. There several reasons why a workflow agent startup or shutdown process can fail:

- The network is down.
- The Content Server containing the workflow agent is down.
- The Content Server projects to a connection broker that is not listed in the dfc.properties of the client running Documentum Administrator.

If the repository is not reachable, the Parameters page displays the Workflow Agent Current Status as Unknown.

**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 237
- **CLEAN_LINKS**, page 238
- **DELETE_REPLICA**, page 238
- **DESTROY_CONTENT**, page 239
- **EXPORT_TICKET_KEY**, page 240
- **GET_PATH**, page 240
- **IMPORT_REPLICA**, page 241
- **IMPORT_TICKET_KEY**, page 242
- **MIGRATE_CONTENT**, page 242
- **PURGE_CONTENT**, page 247
- **REPLICATE**, page 248
- **RESTORE_CONTENT**, page 249
- **SET_STORAGE_STATE**, page 250

The following are database methods:

- **DB_STATS**, page 251
- **EXEC_SQL**, page 252
- **MAKE_INDEX**, page 255
- **DROP_INDEX**, page 251
- **MOVE_INDEX**, page 256
- **FINISH_INDEX_MOVES**, page 252
The following are full-text indexing methods:
- ESTIMATE_SEARCH, page 256
- MARK_FOR_RETRY, page 257
- MODIFY_TRACE, page 258

The following administration methods are trace methods:
- GET_LAST_SQL, page 258
- LIST_RESOURCES, page 259
- LIST_TARGETS, page 260
- MODIFY_TRACE, page 258
- SET_OPTIONS, page 261

The following is the workflow method:
- RECOVER_AUTO_TASKS, page 262
- WORKFLOW_AGENT_MANAGEMENT, page 263

Choosing a file on the server file system

This section describes how to choose a file on the server file system.

To choose a file on the server file system:
1. Navigate to the correct location on the file system.
2. Select the file.
3. Click OK to return to the Parameters page.
Chapter 8

Alias Sets

This chapter contains the following topics:

- Alias sets and aliases, page 267
- Creating or modifying alias sets, page 267
- Viewing or removing aliases, page 268
- Adding or modifying aliases, page 269
- Deleting alias sets, page 270

Alias sets and aliases

An alias set is an object that defines one or more aliases and their corresponding values. An alias is a placeholder for user names, group names, or folder paths. Content Server provides various alias sets that are installed by default. In Documentum Administrator, all alias sets for a repository are located in the Administration > Alias Sets node.

Aliases can be used 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. However, only the owner of the alias set or a superuser can change or delete an alias set. If the server API is used, the constraints are different:

- To change the owner of an alias set, you must be either the owner of the alias set or have superuser privileges.
- To change other properties or to delete an alias set, you must be the owner of the alias set or a user with system administrator or superuser privileges.

Creating or modifying alias sets

Use these instructions to create new alias sets. Any user can create an alias set.
To create an alias set:

1. Navigate to Administration > Alias Set to access the Alias Sets list page.

2. Do one of the following:
   - To create an alias set, select File > New > Alias Set.
     The New Alias Set page displays with the Info tab selected.
   - To view or modify an alias set, select the alias set, then select View > Properties.

3. Enter information on the Info tab of the New Alias Set page, as described in Table 69, page 268.

4. Click Next or select the Aliases tab.

5. Add aliases to the alias set.

6. Click Finish.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>The name of the alias set.</td>
</tr>
<tr>
<td>Description</td>
<td>A description of the alias set.</td>
</tr>
<tr>
<td>Owner</td>
<td>The name of the alias set owner.</td>
</tr>
<tr>
<td></td>
<td>Click Select to select and assign an owner to the alias set.</td>
</tr>
</tbody>
</table>

Table 69. Alias set properties

Viewing or removing aliases

Use these instructions to view or remove aliases from an alias set.

To view or remove an alias:

1. Navigate to Administration > Alias Set to access the Alias Sets list page.

2. Select an alias set, then select View > Properties.
   The Alias Set Properties page displays with the Info tab selected.

3. Click the Aliases tab.
   The aliases and alias properties display:

<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>The name of the alias.</td>
</tr>
<tr>
<td>Category</td>
<td>The category to which the alias belongs.</td>
</tr>
<tr>
<td>Value</td>
<td>The value assigned to the alias.</td>
</tr>
<tr>
<td>Description</td>
<td>A description of the alias.</td>
</tr>
</tbody>
</table>

4. To remove an alias from the alias set, select the alias and click Remove.
5. Click **OK** to save your changes.

**Adding or modifying aliases**

Use these instructions to add an alias to an alias set or modify an existing alias set.
You must be the owner of the alias set or have superuser privileges to add, modify, or delete aliases.

**To add or modify aliases:**
1. Navigate to **Administration > Alias Set** to access the Alias Sets list page.
2. Select an alias set, then select **View > Properties**.
   The Alias Set Properties page displays with the Info tab selected.
3. Click the **Aliases** tab.
4. Do one of the following:
   • To add an alias, click **Add**.
     The New Alias page displays.
   • To modify an existing alias, select the alias, then click **Edit**.
     The Alias page displays.
5. Add or modify the alias properties, as described in **Table 70, page 269**.
6. Click **OK** to save alias additions, modifications, or deletions and return to the Alias Sets list page.

**Table 70. Alias properties**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>The name of the alias. For an existing alias, the name is a read-only value and cannot be modified.</td>
</tr>
<tr>
<td>Category</td>
<td>The category to which the alias belongs. The category can have the following values:</td>
</tr>
<tr>
<td></td>
<td>• Permission Set</td>
</tr>
<tr>
<td></td>
<td>• Cabinet Path</td>
</tr>
<tr>
<td></td>
<td>• Folder Path</td>
</tr>
<tr>
<td></td>
<td>• Group</td>
</tr>
<tr>
<td></td>
<td>• User</td>
</tr>
<tr>
<td></td>
<td>• User or Group</td>
</tr>
<tr>
<td></td>
<td>• Unknown</td>
</tr>
</tbody>
</table>
### Alias Sets Field Description

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Value</td>
<td>For an existing alias, the category is a read-only value and cannot be modified.</td>
</tr>
<tr>
<td>Value</td>
<td>The value for the category property. Click Get Value to select a value from a list of values associated with the category you previously selected.</td>
</tr>
<tr>
<td>Value</td>
<td>If you selected Unknown as the category, you must type a value in the Value field.</td>
</tr>
<tr>
<td>User Category</td>
<td>A user-defined integer value for the Value property. Optional property.</td>
</tr>
<tr>
<td>During DocApp Installation</td>
<td>Select Prompt Alias value to indicate to prompt for the alias value when a Documentum application is installed.</td>
</tr>
<tr>
<td>During DocApp Installation</td>
<td>If the category is a folder path or cabinet path, you can select between prompting for the value during application installation or creating the folder or cabinet if it does not exist.</td>
</tr>
<tr>
<td>Description</td>
<td>A description for the alias.</td>
</tr>
</tbody>
</table>

### Deleting alias sets

Use these instructions to delete an alias set. You must be the owner of the alias set owner or have superuser privileges to delete an alias set. The constraints are different if you are using the API.

**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.
Chapter 9

Formats

This chapter contains the following formats:

- Formats, page 271
- Viewing, creating, or modifying formats, page 271
- Deleting formats, page 273

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. In Documentum Administrator, all formats are located on the Administration > Formats node.

Viewing, creating, or modifying formats

Use the instructions in this section to view, create, or modify formats.

To view, create, or modify a format:

1. Navigate to Administration > Formats to access the Formats list page.
2. Do one of the following:
   - To create a format, select File > New > Format.
     The New Format page displays with the Info tab selected.
   - To modify a format, select the format, then select View > Properties.
     The Format Properties page displays with the Info tab selected.
3. Complete the properties for the new format, as described in Table 71, page 272.
4. Click OK to save the format or Cancel to exit without saving the changes.
<table>
<thead>
<tr>
<th>Field label</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>The name of the format (for example: doc, tiff, or lotmanu).</td>
</tr>
<tr>
<td>Default File Extension</td>
<td>The DOS file extension to use when copying a file in the format into the common area, client local area, or storage.</td>
</tr>
<tr>
<td>Description</td>
<td>A description of the format.</td>
</tr>
<tr>
<td>Com Class ID</td>
<td>The class ID (CLSID) recognized by the Microsoft Windows registry for a content type.</td>
</tr>
<tr>
<td>Mime Type</td>
<td>The Multimedia Internet Mail Extension (MIME) for the content type.</td>
</tr>
<tr>
<td>Windows Application</td>
<td>The name of the Windows application to launch when users select a document in the format represented by the format object.</td>
</tr>
<tr>
<td>Macintosh Creator</td>
<td>Information used internally for managing Macintosh resource files.</td>
</tr>
<tr>
<td>Macintosh Type</td>
<td>Information used internally for managing Macintosh resource files.</td>
</tr>
<tr>
<td>Class</td>
<td>Identifies the classes or classes of formats to which a particular format belongs. The class property works with all search engines.</td>
</tr>
</tbody>
</table>

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**.

Two values are used by the full-text indexing system to determine which renditions of a document are indexed:

- **ft_always**
  All renditions of a document are indexed.

- **ft_preferred**
  If a document has multiple renditions in indexable formats and one format is set to ft_preferred, the rendition in that format is indexed as well as any formats with the class value set to ft_always.

  If more than one rendition of a document is set to ft_preferred, the first rendition processed for indexing is indexed and the other renditions are not.
<table>
<thead>
<tr>
<th>Field label</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Asset Class</td>
<td>Used by applications. Identifies the kind of asset (video, audio, and so on) represented by this format.</td>
</tr>
<tr>
<td>Filename Modifier</td>
<td>The modifier to append to a filename to create a unique file name.</td>
</tr>
<tr>
<td>Default Storage</td>
<td>Identifies the default storage area for content files in this format. Click Select to access the Choose a Storage page.</td>
</tr>
<tr>
<td>Re-Initialize Server</td>
<td>Select to reinitialize the server so changes occur immediately.</td>
</tr>
<tr>
<td>Rich Media</td>
<td>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.</td>
</tr>
<tr>
<td>Hide</td>
<td>Determine whether the format object should appear in the WorkSpace list of formats. Select to hide the object.</td>
</tr>
<tr>
<td>Full-Text Indexing</td>
<td>Select to enable the format for full-text indexing.</td>
</tr>
</tbody>
</table>

### 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 deleted

The Format list page is displayed.
This chapter contains the following topics:

- Managing types, page 275
- Creating or modifying types, page 276
- Selecting a type, page 280
- Deleting types, page 280
- Viewing assignment policies, page 281
- Converting types to shareable object types, page 281
- Converting types to lightweight object types, page 282
- Converting types to shareable and lightweight object types, page 283

Managing types

In Documentum Administrator, types are managed on the Types page under the Administration > Types node. On the Types page, you can filter types by selecting All, DCTM Types, or Custom Types from the list box. Types whose names are displayed as underlined 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 page if the High-Volume Server license is enabled and the Content Server version is 6 or later.

From the Types page, you can:

- 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 syobject 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, associate a different assignment policy with the type.
The Data Model chapter in EMC Documentum Content Server Fundamentals provides more information on types. The EMC Documentum Object Reference Manual provides complete information on the system-defined object types, including the properties of each type.

Creating or modifying types

Use the instructions in this section to create new object types. To create a type, you must have superuser, system administrator, 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.

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 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 create or modify an object type:

1. Navigate to Administration > Types.
   The Types page displays.
2. Do one of the following:
   • To create a type, select File > New > Type.
      The New Type page displays with the Info tab selected.
   • To modify a type, select the type, then select View > Properties > Info.
      The Type Properties page displays with the Info tab selected.
3. Enter or modify the type properties on the Info tab, as described in Table 72, page 276.
4. Click Next to access the Attribute tab.
   A list of the properties inherited from the supertype is displayed.
   On the Attribute page, you can
   • Click Add to add a property to the type.
   • Select a property and click Edit to modify the property.
   • Select a property and click Delete to delete the property. You cannot delete the inherited properties.
5. Click Finish or OK to save your changes.

Table 72. Type properties

<table>
<thead>
<tr>
<th>Field label</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Info tab</td>
<td></td>
</tr>
<tr>
<td>Field label</td>
<td>Value</td>
</tr>
<tr>
<td>---------------------</td>
<td>-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Type Name</td>
<td>The name of the object type. This field is read-only in modify mode.</td>
</tr>
<tr>
<td>Model Type</td>
<td>This field is read-only in modify mode.</td>
</tr>
<tr>
<td></td>
<td>Options are:</td>
</tr>
<tr>
<td></td>
<td>• <strong>Standard</strong>: This is the default and is for heavy types.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Shareable</strong>: Defines a shareable SysObject model type for SysObject supertypes and their subtypes.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Lightweight</strong>: 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 is not be available. If selected, the Parent Type, Materialize, and FullText fields become available and the Super Type Name field is not displayed.</td>
</tr>
<tr>
<td>Super Type Name</td>
<td>The name of the supertype. The default supertype is dm_document. This field is:</td>
</tr>
<tr>
<td></td>
<td>• Not available if the Model Type is Lightweight.</td>
</tr>
<tr>
<td></td>
<td>• Read-only in modify mode.</td>
</tr>
<tr>
<td></td>
<td>Unless you have superuser privileges, you must identify the type’s supertype. If you do have superuser privileges and want to create the type without a Supertype, select NULL as the supertype.</td>
</tr>
<tr>
<td>Default Storage</td>
<td>A default file store for the object type.</td>
</tr>
<tr>
<td>Default Group</td>
<td>A default group for the type. Click <strong>Select Default Group</strong> to access to add or change the default group.</td>
</tr>
<tr>
<td>Default Permission Set</td>
<td>A default permission set for the type. Click <strong>Select Default Permission Set</strong> to add or change the default permission set.</td>
</tr>
<tr>
<td>Field label</td>
<td>Value</td>
</tr>
<tr>
<td>-----------------------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Default Assignment Policy</td>
<td>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. Click the link to access the assignment policy. Use the information in Assignment policies, page 317 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.</td>
</tr>
</tbody>
</table>
| Enable Indexing             | The system displays the Enable Indexing checkbox if:  
  • The type is dm_sysobject or its subtype and you are connected as a superuser to a 5.3 SP5 or later repository. If neither of these conditions is met, the system does not display the checkbox.  
  • 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.  
  • A type is registered and none of its supertypes are registered. The system displays the Enable Indexing checkbox selected and enabled.  
  • A supertype of the type is registered for indexing. The system displays the Enable Indexing checkbox selected but disabled. You cannot clear the checkbox.  

The system does not display the Enable Indexing checkbox when you create a type. You must first create the type and save it.  

If you are registering a particular type for indexing, the system automatically selects all of its subtypes for indexing. When you are 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. |
<table>
<thead>
<tr>
<th>Field label</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Partitioned</td>
<td>Displays whether a type that can be partitioned is or is not partitioned. This field:</td>
</tr>
<tr>
<td></td>
<td>• Does not appear if the type cannot be partitioned.</td>
</tr>
<tr>
<td></td>
<td>• Displays <em>False</em> if the type can be partitioned but is not.</td>
</tr>
<tr>
<td></td>
<td>• Displays <em>True</em> if the type is partitioned.</td>
</tr>
<tr>
<td>Parent Type</td>
<td>This option is available only when creating a type and Model Type is Lightweight. This field is read-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.</td>
</tr>
<tr>
<td>Materialize</td>
<td>This option is available only when creating a type and Model Type is Lightweight. This field is read-only in modify mode. Select one of the following options:</td>
</tr>
<tr>
<td></td>
<td>• <strong>Auto materialize</strong>: 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.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Materialize on request</strong>: 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.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Do not materialize</strong>: 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.</td>
</tr>
<tr>
<td>Full Text</td>
<td>This option is available only when creating a type and Model Type is Lightweight. This field is display-only in modify mode. Select one of the following options:</td>
</tr>
<tr>
<td></td>
<td>• No fulltext: This is the default.</td>
</tr>
<tr>
<td></td>
<td>• Light fulltext: No attributes inherited from the shared parent will be full-text indexed.</td>
</tr>
<tr>
<td></td>
<td>• Full fulltext</td>
</tr>
<tr>
<td>Field label</td>
<td>Value</td>
</tr>
<tr>
<td>------------------</td>
<td>----------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td><strong>Attribute tab</strong></td>
<td></td>
</tr>
<tr>
<td>Attribute Name</td>
<td>The name of the attribute. This field is display-only in modify mode.</td>
</tr>
<tr>
<td>Type</td>
<td>The property type.</td>
</tr>
<tr>
<td>Size</td>
<td>The size of the property, if the property is the String type.</td>
</tr>
<tr>
<td>Inherited</td>
<td>Yes indicates that a property is inherited from a supertype. No indicates that the property is user-defined. You cannot remove a property inherited from the supertype.</td>
</tr>
<tr>
<td>Repeating</td>
<td>If selected, the property is a repeating property.</td>
</tr>
</tbody>
</table>

**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**.

**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.
   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. Knowing the inheritance hierarchy helps with troubleshooting if content files are not saved in the correct storage area for that type.

The page displays a type 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.
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 shareable 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.
Chapter 11

Storage Management

This chapter contains the following topics:

- Storage management areas, page 285
- Storage, page 285
- Assignment policies, page 317
- Migration policies, page 322

Storage management areas

In Documentum Administrator, the Storage Management node is located under the Administration node and includes three main areas:

- Storage
  The storage area contains pages for creating various store types, such as file stores, retention stores (EMC Centera and NetApp SnapLock), blob stores, turbo stores, Atmos stores, VIPR stores, mount point objects, location objects, and storage plug-ins.

- Assignment Policies
  The Assignment Policies area contains pages for creating assignment policies. These pages only appear if the Content Storage Services feature is enabled for the repository.

- Migration policies
  The Migration Policies are contains pages for creating jobs to move content files among storage areas based on user-defined rules and schedules. These pages only appear if the Content Storage Services feature is enabled for the repository.

Storage

The storage area contains information about existing stores and pages for creating various store types. To access the storage area, select Administration > Storage Management > Storage. The Storage list page displays with a list of existing stores and location objects. If a storage system complies with the NFS or UNIX file system or CIFS (on Microsoft Windows) file system protocols and standards,
Documentum can use this storage system. The first ten storage areas in the repository are displayed in the order in which they were created.

A repository can contain the following storage objects:

**Table 73. Repository storage objects**

<table>
<thead>
<tr>
<th>Storage</th>
<th>Icon</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>File Store</td>
<td><img src="image" alt="File Store Icon" /></td>
<td>File stores hold content as files. <strong>File stores, page 288</strong> provides information about file stores.</td>
</tr>
<tr>
<td>Linked Store</td>
<td><img src="image" alt="Linked Store Icon" /></td>
<td>Linked stores do not contain content, but point to the actual storage area, which is a file store. <strong>Linked stores, page 293</strong> provides more information on linked stores.</td>
</tr>
<tr>
<td>Blob Store</td>
<td><img src="image" alt="Blob Store Icon" /></td>
<td>Blob stores store files directly in the repository in a special table. <strong>Blob stores, page 294</strong> provides more information about blob stores.</td>
</tr>
<tr>
<td>Mount Point</td>
<td><img src="image" alt="Mount Point Icon" /></td>
<td>Mount point objects represent directories that are mounted by a client. <strong>Mount points, page 311</strong> provides more information about mount points.</td>
</tr>
<tr>
<td>External File Store</td>
<td><img src="image" alt="External File Store Icon" /></td>
<td>External file stores do not store any content. They point to the actual file system. <strong>External stores, page 297</strong> provides more information about external file stores.</td>
</tr>
<tr>
<td>External Free Store</td>
<td><img src="image" alt="External Free Store Icon" /></td>
<td>External free stores do not store any content. They point to a CD-ROM or user-defined storage. For example, the XML file store is an external free store used specifically to optimize performance with XML content files. <strong>External stores, page 297</strong> provides more information about external free stores.</td>
</tr>
<tr>
<td>External URL Store</td>
<td><img src="image" alt="External URL Store Icon" /></td>
<td>External URL stores do not store any content. They point to a URL. <strong>External stores, page 297</strong> provides more information about external URL stores.</td>
</tr>
<tr>
<td>Plug-in</td>
<td><img src="image" alt="Plug-in Icon" /></td>
<td>Plug-ins are required for access to external stores. <strong>Plug-ins, page 314</strong> provides more information about plug-ins.</td>
</tr>
<tr>
<td>Storage</td>
<td>Icon</td>
<td>Description</td>
</tr>
<tr>
<td>-------------------------</td>
<td>------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>NetApp SnapLock Store</td>
<td><img src="image" alt="Icon" /></td>
<td>The NetApp SnapLock Store is a retention store for content that is retained for a specified time. Retention stores are often used for storing massive amounts of unchanging data, such as email archives or check images. <strong>NetApp SnapLock stores, page 305</strong> provides more information about NetApp SnapLock stores.</td>
</tr>
<tr>
<td>EMC Centera Store</td>
<td><img src="image" alt="Icon" /></td>
<td>The EMC Centera Store is a retention store for content that is retained for a specified time. Retention stores are often used for storing massive amounts of unchanging data, such as email archives or check images. <strong>EMC Centera stores, page 300</strong> provides more information about EMC Centera Stores.</td>
</tr>
<tr>
<td>Atmos Store</td>
<td><img src="image" alt="Icon" /></td>
<td>The Atmos store is a storage system comprised of several distributed services running on hardware nodes connected via a network. The nodes run a collection of services to store, retrieve, categorize, and manage the data in the system or cloud. <strong>Atmos stores, page 308</strong> provides more information about Atmos stores.</td>
</tr>
<tr>
<td>VIPR Store</td>
<td><img src="image" alt="Icon" /></td>
<td>ViPR is a software-defined storage platform that abstracts, pools, and automates a data center’s underlying physical storage infrastructure. It provides a single control plane to data center administrators for heterogeneous storage systems. <strong>ViPR stores, page 309</strong> provides more information about ViPR stores.</td>
</tr>
<tr>
<td>Distributed Store</td>
<td><img src="image" alt="Icon" /></td>
<td>Distributed stores do not contain content, but 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. <strong>Distributed stores, page 295</strong> provides more information about creating, viewing, and modifying distributed stores.</td>
</tr>
<tr>
<td>Location</td>
<td><img src="image" alt="Icon" /></td>
<td>Location objects represent directories or files that are accessed by Content Server. <strong>Locations, page 312</strong> provides more information about locations.</td>
</tr>
</tbody>
</table>
**File stores**

A file store is a directory that contains content files. It is the basic storage type of a repository. Each file store has 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 or you can select the location while creating the file store. In the latter case, Documentum Administrator creates the location object for you.

Creating, viewing, or modifying file stores, page 288 provides information about creating, viewing, or modifying file stores.

**Creating, viewing, or modifying file stores**

Use the instructions in this section to create, view, or modify file stores.

**To create a file store:**

1. Connect to the repository where you want to create a new file store.
2. Navigate to Administration > Storage Management > Storage. The Storage list displays.
3. Do one of the following:
   - Select File > New > File Store to create a new file store. The New File Store - Info page displays.
   - Select the file store to modify, then select View > Properties > Info. The system displays the File Store Properties - Info page.
4. Enter information on the New File Store - Info page to create a file store, or view or modify the information on the File Store Properties - Info page.
   - Some of the fields cannot be modified for an existing file store. Table 74, page 288 describes all file store properties.
5. Click OK to save your changes.

**Table 74. File store properties**

<table>
<thead>
<tr>
<th>Field label</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Info tab</strong></td>
<td></td>
</tr>
<tr>
<td>Name</td>
<td>The name of the file store. The name must be unique within the repository.</td>
</tr>
<tr>
<td>Description</td>
<td>The 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.</td>
</tr>
<tr>
<td>Field label</td>
<td>Description</td>
</tr>
<tr>
<td>-------------------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Location</td>
<td>Select the location on the server host.</td>
</tr>
<tr>
<td><strong>Caution:</strong></td>
<td>Be sure that the storage path you specify does not point to the same physical location as any other file stores. If two file stores use the same physical location, data loss may result.</td>
</tr>
<tr>
<td>Media Type</td>
<td>The media type to store in the storage area. Options are: ◦ Regular Content ◦ Thumbnail Content ◦ Streaming Content Media type cannot be changed for an existing file store.</td>
</tr>
<tr>
<td>Base URL</td>
<td>The base URL used to retrieve content directly from a storage area.</td>
</tr>
<tr>
<td>Encrypted</td>
<td>Indicates if the files store is encrypted. This option is only available in repositories with Trusted Content Services enabled and cannot be changed for an existing file store.</td>
</tr>
<tr>
<td>Make Public</td>
<td>Indicates if the area is accessible to the public with no restrictions.</td>
</tr>
<tr>
<td>Add Extension</td>
<td>Indicates whether the server appends an extension to the file when writing it into the storage area. This option cannot be changed for an existing file store.</td>
</tr>
<tr>
<td>Require Ticket</td>
<td>Indicates whether the server generates a ticket when returning the URL to a content file.</td>
</tr>
<tr>
<td>SurrogateGet Method</td>
<td>Installs a custom SurrogateGet method. This field only displays for an existing file store.</td>
</tr>
<tr>
<td></td>
<td>To install the method, click <strong>Select Method</strong> and browse to the method on the server host file system.</td>
</tr>
<tr>
<td>Offline Get Method</td>
<td>Indicates whether the server uses an offline Get method. This field only displays for an existing file store.</td>
</tr>
<tr>
<td>Status</td>
<td>Select a radio button to change the status of the file store to on line, off line, read-only, or WORM (Write Once Read Many). This field only displays for an existing file store.</td>
</tr>
<tr>
<td>Field label</td>
<td>Description</td>
</tr>
<tr>
<td>---------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Digital Shredding</td>
<td>Select to enable digital shredding. Digital shredding is a security feature that removes deleted content files and their associated content objects. It overwrites the addressable locations of the file with a character, then its complement, and finally a random character. Digital shredding requires a Trusted Content Services license.</td>
</tr>
<tr>
<td>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.</td>
<td></td>
</tr>
<tr>
<td>Content Compression</td>
<td>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. Content compression is a feature that automatically compresses a file 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.</td>
</tr>
<tr>
<td>Content Duplication</td>
<td>Select to enable content duplication checking. This option is only available in repositories with Content Storage 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. Content duplication minimizes the amount of content file duplication in the file store. Content</td>
</tr>
</tbody>
</table>
The Space Info tab only displays for an existing file store.

Active Space/Files

The space used by the file store and the number of files.

Orphaned Space/Files

The amount of orphaned space in the file store and the number of orphaned files.

To move a file store storage area:

You can move an entire file store storage area. For example, to reorganize your hardware, you may need to move a storage area to a different disk.

Use the following procedure to move a file store storage area. The procedure describes how to move an entire storage area. It does not describe how to move individual files from one storage area to another.

1. Log in to the repository.
2. Set the storage area offline.
   
   ```
   EXECUTE set_storage_state
   WITH store = 'filestore_name', offline = TRUE
   ```
3. Copy the files in the storage area to the new location.
   - On Windows:
     ```
     c:\>copy /s /e source_directory target_directory
     ```
   - On Linux:
     ```
     % cp -r -p source_directory target_directory
     ```

   where `source_directory` is the top-level directory in the current storage area and `target_directory` is the new directory for the storage area. If the target directory does not exist when this command is issued, the command creates it and copies the files and subdirectories into it from the source directory.

   If the target directory does not exist when this command is issued, the command copies the source directory (and all files and subdirectories) into the target directory as a subdirectory.

4. Set the `file_system_path` property of the `dm_location` object associated with the file store object to point to the new directory for the storage area.
   ```
   UPDATE "dm_location" OBJECT
   SET "file_system_path" = new_directory_path
   WHERE "object_name" = location_object_name
   ```

   **Note:** In a file store object, the root property contains the object name of the location object associated with the storage area.

5. Reinitialize the server and make the change visible.
6. Put the storage area back online:

   EXECUTE set_storage_state
   WITH store = 'filestore_name', offline = FALSE

   You may remove the old storage area if you have no problems retrieving the contents of documents from the new storage area.

   **Note:** It is recommended to use Documentum Administrator to perform the DQL statements.

---

### Configuring NAS file stores

This section describes the instructions to configure Data Domain and Isilon NAS file stores.

Before configuring, please ensure the following for Windows:

- Content Server host and NAS storage host should be in same domain.
- Domain Administrator only can install Content Server on the Content Server host.

**To configure NAS file stores:**

1. Log in to the Content Server Windows host as the domain administrator.
2. Install Content Server on the Content Server host. The *EMC Documentum Content Server Installation Guide* contains the installation instructions.
3. Once the Content Server installation is complete, you will be prompted to configure the repository using the Content Server Configuration Program. Perform the following steps:
   a. In the configuration options screen, choose **Repository** and click **Next**.
   b. Enter the **installation owner password** where the password is the Domain Administrator’s password and click **Next**.
   c. Choose **Add a new repository** and click **Next**.
   d. Specify a **data directory** for storing content files and indicate whether it resides on a **SAN or NAS device**.
      - For Windows: Data directory path is the CIFS share path of the NAS storage device.
      - For Linux/Unix: NAS storage device NFS share path is mounted on the Linux/Unix host as root and used as the data directory path.

    ```
    root$ mount -t nfs <IP address of DD store> :<shared NFS path><local mount path>
    ```

   **Note:** The data directory must not be a top-level directory on a SAN or NAS device such as `\ip_address`. For SAN or NAS, enter the complete path including a shared device and at least one level of directory. Here is an example of a valid data directory on a SAN or NAS device: `\ip_address\Documentum\data`. The default data directory is `$DOCUMENTUM/data`.

   Click **Next**.
   e. Select **Yes** for the **Is this a NAS or SAN device** option and click **Next**.
   f. Continue with the options in the Content Server Configuration Program and complete it. The *EMC Documentum Content Server Installation Guide* contains the detailed instructions.
Once the Documentum Content Server Configuration Program is complete, the NFS file store share is created.

**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.

Linked stores are not available in a Documentum 6 or later repository. However, linked stores are available in 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. Creating, viewing, or modifying linked stores, page 293 provides information about creating viewing or modifying linked stores.

**Creating, viewing, or modifying linked stores**

Use these instructions to create, view or modify a linked store.

**To create or modify 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. Do one of the following:
   - Click File > New > Linked Store to create a new linked store.
   - Select the linked store you want to view or modify, then select View > Properties > Info. The Info page for a linked store appears.
4. Enter or modify the linked store information on the Info page, as described in Table 75, page 293.
5. Click OK to save your changes.

**Table 75. Linked store properties**

<table>
<thead>
<tr>
<th>Field label</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>The name of the storage object. This name must be unique within the repository.</td>
</tr>
<tr>
<td>Location</td>
<td>The name of the directory containing the logical link.</td>
</tr>
<tr>
<td>Linked Store</td>
<td>The name of the storage area to which the link is pointing.</td>
</tr>
<tr>
<td>Use symbolic links</td>
<td>If selected, symbolic links are used.</td>
</tr>
<tr>
<td>Field label</td>
<td>Value</td>
</tr>
<tr>
<td>------------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Get Method</td>
<td>To install a custom SurrogateGet, click Select Method and browse to the method on the server host file system. This option only appears if you are modifying an existing linked store.</td>
</tr>
<tr>
<td>Offline Get Method</td>
<td>Select to use an offline Get method. This option only appears if you are modifying an existing linked store.</td>
</tr>
<tr>
<td>Status</td>
<td>Select a radio button to change the status of the file store to on line, off line, or read only. This option only appears if you are modifying an existing linked store.</td>
</tr>
</tbody>
</table>

**Blob stores**

The content in a blob store is stored directly in the repository rather than on the host file system of the server. 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.

Creating, viewing, or modifying blob stores, page 294 provides information about creating, viewing, or modifying blob stores.

**Creating, viewing, or modifying blob stores**

Use the instructions in this section to create, view or modify a blob store.

**To create, view, or modify a blob store:**

1. Connect to the repository, where you want to create, view or modify a blob store.
2. Navigate to Administration > File Management > Storage. The Storage list page appears.
3. Do one of the following:
   - To create a blob store, select File > New > Blob Store.
The New Blob Store - Info page displays.

- To view or modify a blob store, select an existing blob store, then select View > Properties > Info.

The Blob Store Properties - Info page displays.

4. Enter information on the New Blob Store - Info page to create a file store, or view or modify the information on the Blob Store Properties - Info page.

Some of the fields cannot be modified for an existing blob store. Table 76, page 295 describes all blob store properties.

5. Click OK to save your changes.

Table 76. Blob store properties

<table>
<thead>
<tr>
<th>Field label</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>The name of the storage object. This name must be unique within the repository and must conform to the rules governing type names.</td>
</tr>
<tr>
<td>Content Type</td>
<td>Valid values are:</td>
</tr>
<tr>
<td></td>
<td>• ASCII</td>
</tr>
<tr>
<td></td>
<td>• 8-bit Characters</td>
</tr>
<tr>
<td>Get Method</td>
<td>To install a custom SurrogateGet, click Select Method and browse to the method on the server host file system. This option only displays for existing blob stores.</td>
</tr>
<tr>
<td>Offline Get Method</td>
<td>Select to use an offline Get method. This option only displays for existing blob stores.</td>
</tr>
<tr>
<td>Status</td>
<td>Select a radio button to change the status of the file store to on line, off line, or read only. This option only displays for existing blob stores.</td>
</tr>
</tbody>
</table>

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 the components must store the same kind of content.

Distributed storage areas are useful when repository users are located in widely separated locations. 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.

The EMC Documentum Distributed Configuration Guide describes how to implement and administer a distributed storage area. The EMC Documentum Object Reference Manual lists the properties defined for the distributed store object type.
Creating, viewing, or modifying distributed stores, page 296 provides information about creating, viewing, or modifying distributed stores.

Creating, viewing, or modifying distributed stores

Use the instructions in this section to create, view, or modify, a distributed store.

**Note:** When a repository is configured to use distributed storage, it cannot be converted back to non-distributed storage.

**To create, view, or modify a distributed store:**

1. Connect to the repository, where you want to create, view or modify a distributed store.
2. Select Administration > File Management > Storage. The Storage list page displays.
3. Do one of the following:
   - To create a new distributed store, select File > New > Distributed Store.
   - To view or modify an existing distributed store, select a distributed store, then select View > Properties > Info.
4. Enter information on the New Distributed Store - Info page to create a file store, or view or modify the information on the Distributed Store Properties - Info page. Some of the fields cannot be modified for an existing distributed store. Table 77, page 296 describes all distributed store properties.
5. Click Finish or OK to save your changes.

**Table 77. Distributed store properties**

<table>
<thead>
<tr>
<th>Field label</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Infotab</strong></td>
<td></td>
</tr>
<tr>
<td>Name</td>
<td>The name of the distributed store. 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.</td>
</tr>
<tr>
<td>Fetch Content Locally Only</td>
<td>Indicates whether the server fetches content locally or from far stores that are not available locally.</td>
</tr>
<tr>
<td>Get Method</td>
<td>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.</td>
</tr>
</tbody>
</table>

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.
<table>
<thead>
<tr>
<th>Field label</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Offline Get Method</td>
<td>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.</td>
</tr>
<tr>
<td>Status</td>
<td>Indicates whether the storage area is on line, off line, or read only. Adamant I teri er the t met th m e  f ar e</td>
</tr>
</tbody>
</table>

**Components tab**

| Add              | Adds stores to the distributed store. Click **Add**. The **Choose a storage** page displays. Select the stores in the left column you want to add and move them to the right column, using the right arrow button. |
| Remove           | Removes stores from the distributed store. Select a store in the store list and click **Remove** to remove the store from the distributed store. |

**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 before you create an external store. The plug-in can run on the server side or client side, although a client-side plug-in could provide better performance. Documentum provides code for sample plug-ins in the DM_HOME/unsupported/plugins directory.

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.

- 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.

Creating, viewing, or modifying external stores, page 298 provides information about creating, viewing, or modifying external stores.

The EMC Documentum XML Store Installation and Administration Guide provides more information about external XML file stores.

Creating, viewing, or modifying external stores

Create the appropriate plug-ins before configuring the external store. Use the instructions in this section to create, view, or modify an external file store, external free store, XML store, or external URL store.

To create, view, or modify an external store:
1. Connect to the repository where you want to create, view, or modify an external store.
2. Navigate to Administration > File Management > Storage.
   The Storage list displays.
3. Do one of the following:
   - To create an external file store, select File > New > External File Store.
     The New External File Store - Info page displays.
   - To create a external free store or XML store, select File > New > External Free Store.
     The New External Free Store - Info page displays.
   - To create an external URL store, select File > New > External URL Store.
     The New External URL Store - Info page displays.
   - To view or modify an existing external store, select the external store, then select View > Properties > Info
     The Info page for the external store displays.
4. Enter information on the associated new external store page to create an external store, or view or modify the information on the associated external store info page.
   Some of the fields cannot be modified for an existing distributed store. Table 78, page 299 describes all distributed store properties.
Table 78. External store properties

<table>
<thead>
<tr>
<th>Field label</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Info tab</strong></td>
<td></td>
</tr>
<tr>
<td>Name</td>
<td>The name of the new external store.</td>
</tr>
<tr>
<td>Windows</td>
<td>Indicates the plug-in that is used on the Windows platform.</td>
</tr>
<tr>
<td>Solaris</td>
<td>Indicates the plug-in that is used on the Solaris platform.</td>
</tr>
<tr>
<td>Aix</td>
<td>Indicates the plug-in that is used on the Aix platform.</td>
</tr>
<tr>
<td>HP-UX</td>
<td>Indicates the plug-in that is used on the HP-UX platform.</td>
</tr>
<tr>
<td>Macintosh</td>
<td>Indicates the plug-in that is used on the Macintosh platform.</td>
</tr>
<tr>
<td>Linux</td>
<td>Indicates the plug-in that is used on the Linux platform.</td>
</tr>
<tr>
<td>HP-UX-Itanium</td>
<td>Indicates the plug-in that is used on the HP-UX-Itanium platform.</td>
</tr>
<tr>
<td>Current Client Root</td>
<td>The name of the location object that represents the default root of the content for executing plug-ins on the client when the mount is not executed. This option is only for external file stores.</td>
</tr>
<tr>
<td>Client Root</td>
<td>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 only available for external file stores.</td>
</tr>
<tr>
<td><strong>Server tab</strong></td>
<td></td>
</tr>
<tr>
<td>Add</td>
<td>The Server tab only displays for external file stores.</td>
</tr>
<tr>
<td>Server</td>
<td>Click Add or select the server on which the external file store resides, then click Edit to access the Choose a server config page.</td>
</tr>
<tr>
<td>Location</td>
<td>The location object that points to the external file store. Click Select Location to select a location object.</td>
</tr>
<tr>
<td>Path</td>
<td>Specifies the file system path to the external file store. The path displays automatically after you selected the location object.</td>
</tr>
</tbody>
</table>

**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.
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.

EMC Centera stores

An EMC Centera store is a retention store for large amounts of unchanging data such as email archives or check images. EMC Centera requires a Content Services for EMC Centera (CSEC) license. CSEC must be enabled during Content Server software installation.

Storage systems made by vendors other than EMC are not supported.

In an EMC Centera store:

- Store metadata values with a piece of content.
- Store files created on Macintosh platforms.
  Both, Content Server and DFC must be on version 6.7 or later and there is no backward compatibility to older versions of Content Server and DFC. Any attempt to store resource forks into a Centera store using either an earlier Content Server or DFC version results in an exception/error message.
- 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.

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.

Content Server supports distributed Centera clusters in 5.3 SP3 and later repositories. The Centera store plug-in must be stored depending on different server locations:

- 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, 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.

Creating, viewing, or modifying EMC Centera stores, page 301 provides information about creating, viewing, or modifying EMC Centera stores.
Creating, viewing, or modifying EMC Centera stores

To create an EMC Centera store, you must know the connection string of the Centera storage system.

To create, view, or modify an EMC Centera store:
1. Connect to the repository, where you want to create, view or modify an EMC Centera store.
2. Select Administration > File Management > Storage.
   The Storage list page displays.
3. Do one of the following:
   • To create an EMC Centera store, select File > New > EMC Centera Store.
   • To view or modify an existing EMC Centera store, select a Centera store, then select View > Properties > Info.
4. Enter information on the New EMC Centera Store - Info page to create a file store, or view or modify the information on the EMC Centera Store Properties - Info page.
   Some of the fields cannot be modified for an existing EMC Centera store. Table 79, page 301 describes all EMC Centera store properties.
5. Click OK to save your changes.

Table 79. EMC Centera store properties

<table>
<thead>
<tr>
<th>Field label</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>The name of the Centera store.</td>
</tr>
<tr>
<td>Description</td>
<td>A description of the EMC Centera store.</td>
</tr>
<tr>
<td>Plug-in Name</td>
<td>Specifies the plug-in that is used for the EMC Centera store. Select one of the following options:</td>
</tr>
</tbody>
</table>

• **Default Plugin:** Sets a null ID (0000000000000000) in the a_plugin_id property of the EMC Centera store object.

• **Select Plugin:** Enables 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 314 to create a new plug-in object with the content of the plug-in object set as follows:

• Windows: %DM_HOME%\bin\emcplugin.dll

• Linux: $DM_HOME/bin/libemcplugin.so
<table>
<thead>
<tr>
<th>Field label</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Storage Parameters</td>
<td>Specifies the storage parameters, such as the connection string, C-clip buffer size, and embedded blob storage. Click <strong>Edit</strong> to configure storage parameters, as described in <a href="#">Defining the storage parameters for an EMC Centera store, page 303</a>.</td>
</tr>
<tr>
<td>Enable Content Compression</td>
<td>Specifies whether content compression is used. Select this option to compress all content in the store. Compression cannot be modified for existing Centera stores.</td>
</tr>
<tr>
<td>Configure Retention Information</td>
<td>Enables content retention. Content retention cannot be modified for existing Centera stores.</td>
</tr>
<tr>
<td>Retention Attribute Name</td>
<td>The name of the retention attribute. The value must <em>not</em> be one of the values specified as a content attribute name. The retention attribute name cannot be modified for an existing Centera store.</td>
</tr>
<tr>
<td>Fixed Retention</td>
<td>Specifies a fixed value for the retention property value, as follows:</td>
</tr>
<tr>
<td></td>
<td>• <strong>Choose a retention period:</strong> Sets a period of days as the retention period for all content in the Centera store. Enter the date and time of the retention date.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Choose default retention days:</strong> Select and then type the number of retention days.</td>
</tr>
<tr>
<td></td>
<td>Both default retention date and default retention days can be specified. If both are specified, the default retention days takes precedence over default retention date. If default retention date is selected but no value is specified, the system ignores the retention date option.</td>
</tr>
<tr>
<td>Event Based Retention</td>
<td>When Configure Retention Information is selected, the system automatically selects and inactivates this checkbox to prevent changing the event based retention option status.</td>
</tr>
</tbody>
</table>
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. On the *Info* tab of the EMC Centera Store Properties, scroll to the *Storage Parameters* field and click *Edit*.
   The Storage Parameters page displays.
2. In the *Enter new value* field, type the connection string for the EMC Centera storage system. The connection string has the following format

   \[IP\_address\|hostname\{,IP\_address\|hostname\}?Centera\_profile\]

   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 and must begin with “path=”. The path must be accessible from the Content Server host machine and the specified directory must be readable by the Content Server installation owner.

   The following example describes a connection string with multiple Centera profiles:

   \[10.241.35.27,10.241.35.28\?name=profA,secret=foo,10.241.35.27,10.241.35.28\?name=profB,secret=bar,10.241.35.110,10.241.35.111\?path=C:\Temp\auth.xml\]

In the following example, the SDK parses the passed-in connection string with the resulting elements going in the *outConnectionStrings* array, as follows:

   \[
   \begin{align*}
   \text{outConnectionStrings}[0] &= 10.241.35.27\?name=profA,secret=foo \\
   \text{outConnectionStrings}[1] &= 10.241.35.28\?name=profA,secret=foo \\
   \text{outConnectionStrings}[2] &= 10.241.35.27\?name=profB,secret=bar \\
   \text{outConnectionStrings}[3] &= 10.241.35.28\?name=profB,secret=bar \\
   \text{outConnectionStrings}[4] &= 10.241.35.110\?path=C:\Temp\auth.xml \\
   \text{outConnectionStrings}[5] &= 10.241.35.111\?path=C:\Temp\auth.xml
   \end{align*}
   \]
The following rules apply to the syntax of a connection string with multiple profiles:

- The IP address position must precede the listing of credentials and/or path for that profile.
- If the connection string includes a path that does not use the path= prefix but points to a PEA file and a set of credentials, the path must precede the credentials. Conversely, when using the path= prefix, there is no restriction as to where the path appears in the connection string in relation to the set of credentials.
- The credentials that appear in a connection string override those that are held in a PEA file.
- It is best practice to use the optional path= prefix hint to specify the path to a PEA file, to avoid confusion when evaluating the connection string. Do not mix credential data in a connection string.

If configuring Centera clusters, the connection string format identifies primary and secondary Centera clusters for one or more Content Servers:

```
server_config_name="primary=cluster_id[,cluster_id],secondary=cluster_id[,cluster_id]?Centera_profile"
```

where:

- The primary `cluster_id` is the name or IP address of the Centera cluster to which the Content Server writes.
- The secondary `cluster_id` is the name or IP address of the Centera cluster from which the Content Server reads 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.

3. Click **Add** to move the value to the **Storage Parameters** section.
4. Enter more storage parameters, as necessary.

For example:

- 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
  ```

  If embedded blob use has been enabled and content is written to a compressed Centera store, Content Server writes the content as linked blob if the original content size is greater than the embedded blob threshold. This restriction still applies if the eventual compressed content size is less than or equal to the embedded blob threshold. If the original content size is less than the embedded blob threshold, the content is stored as embedded blob.

- 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

- To change the maximum number of socket connections that the Centera SDK can establish with the Centera host, enter the following parameter:

  pool_option:max_connections:integer

  where integer is an integer number from 1 to 999 specifying the maximum socket connections. By default, the maximum number of socket connections is 99 on Windows platforms, and 1 on UNIX and Linux platforms.

5. Use the up and down arrows to sort the storage parameters.

  **Caution:** If you have entered multiple parameters, the EMC Centera connection string must be in the first position.

6. When finished, click **OK**.

**Defining EMC Centera store content attributes**

EMC Centera stores allow you to save up to 62 metadata values with each piece of content saved in the system.

**To define the content attributes saved in an EMC Centera store:**

1. On the **Info** tab of the **EMC Centera Store Properties**, scroll to the Content Attribute section and click **Add**.
   
   The **Content Attribute** page displays.

2. 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.

3. Type a description.

4. Click **OK**.

5. Repeat step 1 through 4 to configure more attributes, if applicable.

**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

Creating, viewing, or modifying NetApp SnapLock stores, page 306 provides information about creating, viewing, or modifying NetApp SnapLock stores.

**Creating, viewing, or modifying NetApp SnapLock stores**

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, view, or modify a NetApp SnapLock store:**

1. Connect to the repository, where you want to create, view or modify NetApp SnapLock store.
2. Select **Administration > File Management > Storage**.
   The **Storage** list page displays.
3. Do one of the following:
   - To create an NetApp SnapLock store, select **File > New > NetApp SnapLock Store**.
   - To view or modify an existing NetApp SnapLock store, select a NetApp SnapLock store, then select **View > Properties > Info**.
4. Enter information on the **New NetApp SnapLock Store - Info** page to create a NetApp SnapLock store, or view or modify the information on the **NetApp SnapLock Store Properties - Info** page.
   Some of the fields cannot be modified for an existing NetApp SnapLock store. **Table 80, page 306** describes all NetApp SnapLock store properties.
5. Click **OK** to save your changes.

**Table 80. NetApp SnapLock store properties**

<table>
<thead>
<tr>
<th>Field label</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>The name of the NetApp SnapLock store.</td>
</tr>
<tr>
<td>Description</td>
<td>A description of the NetApp SnapLock store.</td>
</tr>
<tr>
<td>Field label</td>
<td>Description</td>
</tr>
<tr>
<td>--------------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Plug-in Name</td>
<td>The name of the plug-in for the NetApp SnapLock store. Options are:</td>
</tr>
<tr>
<td></td>
<td>• Default Plugin: Select to set a null ID (0000000000000000) in the a_plugin_id property of the NetApp SnapLock store object.</td>
</tr>
<tr>
<td></td>
<td>• Select Plugin: Select to use the default Snaplock Connection plug-in.</td>
</tr>
<tr>
<td></td>
<td>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 314 to create a new plug-in object with the content of the plug-in object set as follows:</td>
</tr>
<tr>
<td></td>
<td>— Windows: %DM_HOME%\bin\emcplugin.so</td>
</tr>
<tr>
<td>Snaplock Volume Path</td>
<td>The directory path of the NetApp SnapLock storage system.</td>
</tr>
<tr>
<td>Enable Content Compression</td>
<td>Specifies whether content compression is used. Select this option to compress all content in the store.</td>
</tr>
<tr>
<td></td>
<td>Compression cannot be modified for existing NetApp SnapLock stores.</td>
</tr>
<tr>
<td>Configure Retention Information</td>
<td>Enables content retention.</td>
</tr>
<tr>
<td></td>
<td>Content retention cannot be modified for existing NetApp SnapLock store.</td>
</tr>
<tr>
<td>Retention Attribute Name</td>
<td>The name of the retention attribute. The value must not be one of the values specified as a content attribute name.</td>
</tr>
<tr>
<td></td>
<td>The retention attribute name cannot be modified for an existing NetApp SnapLock store.</td>
</tr>
</tbody>
</table>
### Fixed Retention

Specifies a fixed value for the retention property value, as follows:

- **Choose a retention period**: Sets a period of days as the retention period for all content in the NetApp SnapLock store. Enter the date and time of the retention date.

- **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 takes precedence over default retention date. If default retention date is selected but no value is specified, the system ignores the retention date option.

### 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.

### Application Provides Retention

Requires that a client application supplies the retention date when content is saved to the NetApp SnapLock store.

---

### Atmos stores

An Atmos store is an EMC software storage system that consists of several distributed services running on a network of connected hardware nodes. Each node is attached to one more disk enclosures. The nodes run a collection of services to store, retrieve, categorize, and manage the data in the system or cloud.

Content Server uses the ACS connector to communicate with the Atmos store. The ACS module supports storing and retrieving of content through an HTTP interface.

Creating, viewing, or modifying Atmos stores, page 308 provides information about creating, viewing, or modifying Atmos stores.

### Creating, viewing, or modifying Atmos stores

Use these instructions to create and manage Atmos stores.

**To create, view, or modify an Atmos store:**

1. Connect to the repository, where you want to create, view or modify an Atmos store.
2. Select Administration > Storage Management > Storage.
   
   The Storage list page displays.
3. Do one of the following:
   • To create an Atmos store, select File > New > Atmos Store.
   • To view or modify an existing Atmos store, select a Atmos store, then select View > Properties > Info.
4. Enter information on the New Atmos Store - Info page to create an Atmos store, or view or modify the information on the Atmos Store Properties - Info page.
   Some of the fields cannot be modified for an existing Atmos store. Table 81, page 309 describes all Atmos store properties.
5. Click OK to save your changes.

Table 81. Atmos store properties

<table>
<thead>
<tr>
<th>Field label</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>The name of the Atmos store. The name must be unique within the system. The name of an existing Atmos store cannot be modified.</td>
</tr>
<tr>
<td>URL</td>
<td>The URL the server uses to communicate with the Atmos store.</td>
</tr>
<tr>
<td>Full Token ID</td>
<td>A combination of subtenant ID and a UID within that subtenant, both in the Atmos system that is being targeted. The format is subtenant ID/UID.</td>
</tr>
<tr>
<td>Shared Secret</td>
<td>The password of the user accessing the Atmos store.</td>
</tr>
</tbody>
</table>

Managing authentication — The Web service uses a combination of the Token ID, and other request headers to produce a signature that authenticates the user accessing the web service. It uses a combination of various pieces of the message to validate the identity of the sender, integrity of the message, and non-repudiation of the action. The Token ID that you received via e-mail from the portal agent administrator consists of the subtenant ID, and the UID separated by a slash (/). The subtenant ID is a randomly generated, 32 character alphanumeric string, which is unique to each customer. The UID, however, is unique to a web-based application. The UID, which appears after the slash, is comprised of a portion of the customer name, and a randomly generated string. For example, if the customer name is ‘ACME’, then the UID string appends the additional random characters. The whole Token ID contains 53 uppercase characters including the slash, as shown in the following example: 5f8442b515ec402fb4f39ffab8c8179a/ACME03GF52E8D8E581B5

To complete the authentication operation, you must generate a signature using the shared secret, which is associated with the UID. The shared secret is a value generated by the EMC Storage Utility Agent responsible for managing this application. The shared secret appears in the same e-mail message that contains the Token ID. The following sample represents a typical shared secret: MBqhz5zhZJCQHE9U4RBK9ze3K7U=

ViPR stores

ViPR is a software-defined storage platform that abstracts, pools, and automates a data center’s underlying physical storage infrastructure. It provides a single control plane to data center administrators for heterogeneous storage systems. Above the control plane, administrators can
deploy ViPR Services (Object, HDFS, and Block Services) on array- and commodity-based storage that enable users to:

- Use ViPR file-managed storage as an object store
- Perform analytics on ViPR-managed storage
- Dynamically provision block commodity storage

ViPR enables software-defined data centers by providing the following features:

- Storage automation capabilities for multi-vendor block and file storage environments (control plane or ViPR Controller).
- Object data management and analytic capabilities through ViPR Object and HDFS Services, which creates a unified pool (bucket) of data across file shares and commodity servers (data path).
- Management of multiple data centers in different locations with single sign-on data access from any data center.
- Data replication between geographically dispersed data centers to protect against data center failures with active-active functionality.

Creating, viewing, or modifying VIPR stores, page 310 provides the detailed information.

Creating, viewing, or modifying VIPR stores

Before creating, viewing, or modifying VIPR stores

- Install the license for ViPR Object on ViPR, including Amazon S3.
- Enable data services for object-based storage services and ensure that the Amazon S3 store is accessible.
- Create a bucket for data services to be used by the Content Server.

To create, view, or modify VIPR store:

1. Connect to the repository, where you want to create, view, or modify the VIPR store.
2. Select Administration > Storage Management > Storage.
   The Storage list page appears.
3. Do one of the following:
   - To create a VIPR store, select File > New > VIPR Store.
   - To view or modify an existing VIPR store, select a VIPR store, then select View > Properties > Info.

Some of the fields for an existing VIPR store cannot be modified. Table 82, page 311 describes all VIPR store properties.
4. Click OK to save the changes.
Table 82. VIPR store properties

<table>
<thead>
<tr>
<th>Field label</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>The name of the VIPR store. The name must be unique within the system. The name of an existing VIPR store cannot be modified.</td>
</tr>
<tr>
<td>URL</td>
<td>The URL that the server uses to communicate with the VIPR store. The URL format is <a href="http://xx.xx.xx.xx:9020/">http://xx.xx.xx.xx:9020/</a>&lt;bucket-name&gt;. For example, <a href="http://10.31.4.172:9020/csstore">http://10.31.4.172:9020/csstore</a></td>
</tr>
<tr>
<td>Access Key ID</td>
<td>The user name of the user accessing the VIPR store. Use the ViPR Tenant Owner as the Access Key ID.</td>
</tr>
<tr>
<td>Shared Secret</td>
<td>The password of the user accessing the VIPR store. Use the Object Access Key as the Shared Secret.</td>
</tr>
</tbody>
</table>

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.

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 for which you want to create or modify a mount point.
2. Select Administration > File Management > Storage. The Storage list page displays.
3. Do one of the following:
   • To create an mount point, select File > New > Mount Point.
   • To view or modify an existing mount point, select the mount point, then select View > Properties > Info.
4. Enter information on the New Mount Point - Info page to create a mount point, or view or modify the information on the Mount Point Properties - Info page, as described in Table 83, page 312.
5. Click OK to save your changes.
### Table 83. Mount point properties

<table>
<thead>
<tr>
<th>Field label</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>The name of the mount point object. Some names, such as “events” or “common,” are reserved for Content Server use.</td>
</tr>
<tr>
<td>Host Name</td>
<td>The hostname for the machine on which this directory resides.</td>
</tr>
<tr>
<td>File System Path</td>
<td>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.</td>
</tr>
<tr>
<td></td>
<td>For example, if the server is on a Windows NT machine, the location must be expressed as a Windows NT path.</td>
</tr>
<tr>
<td>Caution:</td>
<td>Be sure that the combination of the host and path you specify does not point to the same physical location as any other file stores. If two file stores use the same physical location, data loss may result.</td>
</tr>
<tr>
<td>Security</td>
<td>The security level for this directory location. Options are:</td>
</tr>
<tr>
<td></td>
<td>• Public Open</td>
</tr>
<tr>
<td></td>
<td>• Public</td>
</tr>
<tr>
<td></td>
<td>• Private</td>
</tr>
<tr>
<td></td>
<td>The default value is Private.</td>
</tr>
<tr>
<td>Unix Preferred Alias</td>
<td>Set to the directory name used to mount the directory.</td>
</tr>
<tr>
<td>Macintosh Preferred Alias</td>
<td>Set to the volume name chosen for the mounted directory.</td>
</tr>
<tr>
<td></td>
<td>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.</td>
</tr>
<tr>
<td>Windows Preferred Alias</td>
<td>Set to the alias drive letter used to mount the directory.</td>
</tr>
<tr>
<td></td>
<td>For example, t:\ or k:.</td>
</tr>
<tr>
<td>Comments</td>
<td>Enter any comments about the mount point.</td>
</tr>
</tbody>
</table>

### 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.

*Creating or modifying locations, page 313* provides information on creating or modifying locations.
Creating or modifying locations

A location object contains a file system location for a specific file or directory. The server uses the information in location objects to find the files and directories that it needs for successful operation. 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. Do one of the following:
   - To create a new location, select File > New > Location.
   - To modify an existing location, select the location, and then select View > Properties > Info.
4. Enter information on the New Location-Info page to create a location object, or view or modify the information on the Location Properties - Info page, as described in Table 84, page 313.
5. Click OK to save your changes.

Table 84. Location object properties

<table>
<thead>
<tr>
<th>Field label</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>The name of the location object. Some names, such as &quot;events&quot; or &quot;common,&quot; are reserved for Content Server use.</td>
</tr>
<tr>
<td>Choose a Mount Point for this Location</td>
<td>Identifies the mount point underneath which this location resides. Use the name of the mount point object that describes the mount point.</td>
</tr>
<tr>
<td>Mount Point Path</td>
<td>Specifies the mount point path. Valid values are:</td>
</tr>
<tr>
<td></td>
<td>• Existing: Uses the current mount point path. Select Null to specify that the mount point is not shared, or select share to use this mount point as a shared mount point.</td>
</tr>
<tr>
<td></td>
<td>• Create Mount Point Path: Select to create a mount point path, then click Select Path to browse to a mount point on the file system.</td>
</tr>
</tbody>
</table>
### Field label | Value
---|---
Path | Specifies the file system or UNC path.  
  - **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.  
  - **UNC**: Indicates the UNC path.  
  
  **Caution**: Be sure that the combination of the mount point and path you specify does not point to the same physical location as any other file store. If two file stores use location objects that point to the same physical location, data loss may result.
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:  
  - publicopen  
  - public  
  - private  
  
  If the security type is not set, the default value is the security level of the referencing object, such 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. Documentum provides code for sample plug-ins in the DM_HOME/unsupported/plugins directory. The sample plug-ins are examples and are not supported by EMC Documentum.

The API interface between the shared library or DLL and the server consists of C functions for the plug-in library.

[Creating or modifying plug-ins, page 314](#) provides information on creating or modifying plug-ins.

### 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. Do one of the following:
   - To create a new plug-in, select **File > New > Plug-in**.
   - To modify an existing plug-in, select the correct plug-in and then select **View > Properties > Info**.
4. Enter information on the **New Plug-in Info** page to create a plug-in, or view or modify the information on the **Plug-in Properties - Info** page, as described in **Table 85, page 315**.
5. Click **OK** to save your changes.

**Table 85. Plug-in properties**

<table>
<thead>
<tr>
<th>Field label</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>The name of the plug-in object.</td>
</tr>
<tr>
<td>Hardware Platform</td>
<td>Specifies one or more hardware platforms on which the plug-in can run.</td>
</tr>
<tr>
<td></td>
<td>Click <strong>Edit</strong> to access the <strong>Hardware Platforms</strong> page. Enter the</td>
</tr>
<tr>
<td></td>
<td>hardware type in the <strong>Enter a new value</strong> field, then click <strong>Add</strong>.</td>
</tr>
<tr>
<td></td>
<td>When all types are entered, click <strong>OK</strong>.</td>
</tr>
<tr>
<td>Operating System</td>
<td>Specifies one or more operating systems on which the plug-in can run.</td>
</tr>
<tr>
<td></td>
<td>Click <strong>Edit</strong> to access the <strong>Host Machine</strong> page. Enter the</td>
</tr>
<tr>
<td></td>
<td>operating system in the <strong>Enter a new value</strong> field, then click</td>
</tr>
<tr>
<td></td>
<td><strong>Add</strong>. When all operating systems are entered, click <strong>OK</strong>.</td>
</tr>
<tr>
<td>Type</td>
<td>Select a file type. Options are:</td>
</tr>
<tr>
<td></td>
<td>• DLL (Windows)</td>
</tr>
<tr>
<td></td>
<td>• SO (Linux)</td>
</tr>
<tr>
<td></td>
<td><strong>Note</strong>: The <strong>SL (HP-UX)</strong> file type is available only for pre-7.0</td>
</tr>
<tr>
<td></td>
<td>repositories.</td>
</tr>
<tr>
<td>Usage</td>
<td>Type a comment on how the plug-in is used.</td>
</tr>
</tbody>
</table>

**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.

**Setting or updating a retention date or retention period**

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.

Assignment policies

Assignment policies are sets of rules that DFC-based applications apply to determine the correct file store or retention store for each new content file added to the repository. Assignment policies require a Content Storage Services (CSS) license. Any client application built on DFC applies assignment policies automatically if CSS is enabled in the repository.

Assignment policies can only be applied to the SysObject type and its subtypes, and are represented in the repository by persistent objects. A particular object type can have only one associated assignment policy. When a new content file is added to the repository, the assignment policy engine determines whether the object type of the file has an active associated assignment policy. If there is no active assignment policy for the type, the assignment policy engine determines whether the supertype of the object has an active associated assignment policy. If there is an active assignment policy for the file type or a supertype, the system applies the policy and stores the file accordingly. If no policy is found or if none of the rules match in an applicable policy, the system uses the default algorithm to determine the correct storage area. If none of the rules match in the applicable assignment policy, the policy engine does not further search the type hierarchy.

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 rules
  Standard rules determine storage area based only on the object format and content size. Standard rules can have one to five criteria.

• Custom rules
  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. There are no restrictions on the number of conditions in a custom rule. The properties and values are specified using methods, such as getString(), getInt(), or getRepeatingString(). Custom rules follow the Java syntax for any conditional statements in the rule. Custom assignment policy rule examples, page 321 provides custom rule examples.

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’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. An assignment policy is applied when

• A content file is first saved or imported into the repository.
• A new version of a document is created, because versioning creates a new content file.
• 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.

• An existing document is modified and saved as the same version of the document.

Assignment policies are not applied or enforced under the following conditions:
• 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 properties of an existing documents are modified and saved the changes without checking out and versioning the document. The content is saved into its current storage location.

• 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.

• The content is associated with storage policies.

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 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.

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.

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.

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

Creating, viewing, or modifying 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, view, or modify an assignment policy:
1. Connect to a repository and navigate to Administration > Storage Management > Assignment Policies.
   
The Assignment Policies page displays with all assignment policies that are currently available.
2. Do one of the following:
   - To create an assignment policy, click File > New > Assignment Policy.
   - To view or modify an assignment policy, select the assignment policy, then click View > Properties > Info.
3. Enter or modify the properties and rules for the assignment policy, as described in Table 86, page 319.
4. Click Finish to create the policy or Cancel to exit without creating the policy.

Table 86. Assignment policy properties

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>The name and a description for the assignment policy. The name must be unique in the repository and can be modified after the policy is saved.</td>
</tr>
<tr>
<td>Description</td>
<td>A description of the policy. Optional property.</td>
</tr>
<tr>
<td>Status</td>
<td>Specifies whether the assignment policy is active. 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.</td>
</tr>
<tr>
<td>Field</td>
<td>Description</td>
</tr>
<tr>
<td>-------</td>
<td>-------------</td>
</tr>
<tr>
<td>Validate all of the rules defined for this policy</td>
<td>Validates the rules for the policy if the policy is active. The default is selected. If the policy is created in the active state, the checkbox is selected and grayed out. If the policy is created in the inactive state, optionally clear the checkbox.</td>
</tr>
<tr>
<td>Object types</td>
<td>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. Click Select then select the object types to which the policy applies and click &gt;.</td>
</tr>
<tr>
<td>Create/Edit Rules</td>
<td>Specifies the rules for storing content.</td>
</tr>
<tr>
<td>Standard Rule</td>
<td>The Standard Rule option is selected by default. To create a custom rule, select the Custom Rule option. 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. Create or edit rules using the If and Then operands and drop-down lists to specify formats, content size, and storage areas.</td>
</tr>
<tr>
<td>Add Criteria</td>
<td>Click to add additional conditions to the rule. A standard rule can have up to five criteria.</td>
</tr>
<tr>
<td>Insert Rule</td>
<td>Click to insert the completed rule.</td>
</tr>
<tr>
<td>Cancel Rule</td>
<td>Click to delete text that has been entered in the text box.</td>
</tr>
<tr>
<td>Custom Rule</td>
<td>Type the custom rule in the text box. <strong>Custom assignment policy rule examples, page 321</strong> provides more information on custom rules and examples of custom rule syntax.</td>
</tr>
<tr>
<td>Policy Rules</td>
<td>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.</td>
</tr>
</tbody>
</table>
Modifying the permissions of an assignment policy

Use these instructions to modify the permissions of an assignment policy. An assignment policy 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.

Custom assignment policy rule examples

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 11-1. 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 the correct and required syntax.

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 an assignment policy with an object type:

1. Connect to a repository and navigate to Administration > Storage Management > Assignment Policies.
   The Assignment Policies page displays with all assignment policies that are currently available.
2. Select the assignment policy you want to associated with an object type, then click View > Properties > Info.
3. Click the Select link in the Object Types section to access the Choose a type page.
4. Select the object type(s), click the add arrow, then click OK.
5. Click OK.

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.

Migration policies

Migration policies move content files from one storage area to another, based on the rules (conditions) defined in 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).

Migration policies are jobs that execute 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.
Creating, viewing, or modifying migration policies

Migration policies can be created and used only in repositories where Content Storage Services is enabled.

**To create, view, or modify migration policies:**

1. Connect to a repository and select Administration > Storage Management > Migration Policies. The Migration Policies page displays.

2. From the Migration Policies page, do one of the following:
   - To create a migration policy, select File > New > Migration Policy. The New Migration Policy page displays with the Info tab selected.
   - To view or modify a migration policy, select the policy, then select View > Properties > Info. The Migration Policy Properties page displays with the Info tab selected.

3. Enter information on the Info tab of the New Migration Policy or Migration Policy Properties page, as described in Table 87, page 323.

4. Click Next or click the Schedule tab to enter migration policy scheduling information, as described in Configuring a migration policy schedule, page 324.

5. Click Next or click the Rules tab to enter migration policy rules, as described in Configuring migration policy rules, page 324.

6. Click Next or click the SysObject tab to enter SysObject information, as described in Table 90, page 326.

7. Click Finish.

**Table 87. Migration policy Info tab properties**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>The name of the job. Mandatory property.</td>
</tr>
<tr>
<td>Job Type</td>
<td>The type of job. Optional property. The default value is Content.</td>
</tr>
<tr>
<td>Trace Level</td>
<td>The trace level from 0 (no tracing) to 10 (a debugging level of tracing).</td>
</tr>
<tr>
<td>Designated Server</td>
<td>The server on which the migration policy is run. Select a server from the drop-down list. The list displays each registered servers. The default value is Any Running Server.</td>
</tr>
<tr>
<td>State</td>
<td>Specifies whether the policy is active or inactive. The default value is Active.</td>
</tr>
<tr>
<td>Options</td>
<td></td>
</tr>
<tr>
<td>Deactivate on Failure</td>
<td>Select to deactivate the job after a run fails to execute correctly.</td>
</tr>
</tbody>
</table>
Configuring a migration policy schedule

The migration policy schedule determines when the migration job is executed.

**Table 88. Migration policy Schedule tab properties**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Next Run Date and Time</td>
<td>Specifies the next start date and time for the job. The default is the current date and time.</td>
</tr>
<tr>
<td>Repeat</td>
<td>Specifies the time interval in which the job is repeated.</td>
</tr>
<tr>
<td>Frequency</td>
<td>Specifies how many times the job is repeated.</td>
</tr>
<tr>
<td></td>
<td>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.</td>
</tr>
<tr>
<td>End Date and Time</td>
<td>Specifies the end date and time for the job.</td>
</tr>
<tr>
<td></td>
<td>The default end date is 10 years from the current date and time.</td>
</tr>
<tr>
<td>After</td>
<td>Specifies the number of invocations after which the job becomes inactive.</td>
</tr>
</tbody>
</table>

Configuring migration policy rules

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.

Specify the migration policy rules, as described in Table 89, page 324.

**Table 89. Migration policy Rules tab properties**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Selected Objects</td>
<td>Creates a migration rule based on preset values, such as format, creation date, modification date, access date, or size.</td>
</tr>
<tr>
<td>Simple selection</td>
<td>Creates a migration rule based on preset values, such as format, creation date, modification date, access date, or size.</td>
</tr>
<tr>
<td>Field</td>
<td>Description</td>
</tr>
<tr>
<td>----------------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Move objects where</td>
<td>Specifies which objects to move. Select one of the criteria from the drop-down list, as follows:</td>
</tr>
<tr>
<td></td>
<td>• <strong>format</strong>: Migrates objects of a particular format. Click Select and then select the correct format.</td>
</tr>
<tr>
<td></td>
<td>• <strong>created</strong>: Migrates objects according to creation date.</td>
</tr>
<tr>
<td></td>
<td>• <strong>modified</strong>: Migrates objects according to their modification date.</td>
</tr>
<tr>
<td></td>
<td>• <strong>accessed</strong>: Migrates objects according to the date they were last accessed.</td>
</tr>
<tr>
<td></td>
<td>• <strong>size</strong>: Migrates objects according to their size in bytes. Enter the number of bytes.</td>
</tr>
<tr>
<td></td>
<td>For the created, modified and accessed operands, the number of days is always in relation to the date the job is scheduled to run. Valid operands are:</td>
</tr>
<tr>
<td></td>
<td>• <strong>Exactly</strong>: Migrates objects modified exactly the number of days before.</td>
</tr>
<tr>
<td></td>
<td>• <strong>More than</strong>: Migrates objects modified more than the number of days before.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Less than</strong>: Migrates objects modified less than the number of days before.</td>
</tr>
<tr>
<td>Renditions to include</td>
<td>Specifies whether to migrate <strong>Primary</strong> or <strong>Secondary</strong> renditions or both. The rendition option is only available in conjunction with the created, modified, or accessed selection criteria.</td>
</tr>
<tr>
<td>DQL query selection</td>
<td>Creates a migration rule based on a DQL query. Custom rules can select content to be migrated from dm_sysobject, its subtypes, and dmr_content objects.</td>
</tr>
<tr>
<td>Move specified type</td>
<td>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.</td>
</tr>
<tr>
<td>Move content objects only</td>
<td>Select to migrate the content associated with content objects (dmr_content).</td>
</tr>
<tr>
<td>Where</td>
<td>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.</td>
</tr>
<tr>
<td>Renditions to include</td>
<td>If you selected <strong>Move specified types</strong>, select to migrate <strong>Primary</strong> or <strong>Secondary</strong> renditions or both.</td>
</tr>
</tbody>
</table>

**Move options**
### Field | Description
--- | ---
Target Store | The destination storage area to which the content files migrate. Select a store from the drop-down list. The list includes file stores and retention stores (EMC Centera and NetApp SnapLock).
Batch Size | The number of content files to include in a single transaction during the migration operation. The default value is 500.
Maximum Count | The maximum number of content files to transfer. To specify an unlimited number of documents, type a zero [0] or leave the field blank.
Content Migration Threads | The number of internal sessions to use to execute the migration policy. The default value is 0, indicating that migration executes sequentially.

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).

### Configuring migration policy SysObject information

The SysObject information typically consists of metadata associated with the object.

#### Table 90. Migration policy SysObject tab properties

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Title</td>
<td>The title of the object.</td>
</tr>
<tr>
<td>Subject</td>
<td>The subject of the object.</td>
</tr>
<tr>
<td>Keywords</td>
<td>Keywords that describe the object. Click Edit to access the Keywords page. Enter a new keyword in the Enter new value box and click Add.</td>
</tr>
<tr>
<td>Authors</td>
<td>The author of the object. Click Edit to access the Authors page. Type a new author in the Enter new value box and click Add.</td>
</tr>
<tr>
<td>Owner Name</td>
<td>The owner of the object. Click Edit to access the Choose a user page and select an owner.</td>
</tr>
<tr>
<td>Show more</td>
<td>Click to view more SysObject properties of the migration policy.</td>
</tr>
</tbody>
</table>
Viewing migration policy job reports

A job report contains information about the job, such as when the job was started and whether the job ran successfully.

To view a migration policy job report:
1. Connect to a repository and select Administration > Storage Management > Migration Policies. The Migration Policies page displays.
2. Select the policy for which you want to view the report, then select View > Report. The Report page displays.

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 page displays. 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 12

Content Delivery

This chapter contains the following topics:

• Content delivery services, page 329
• Locating content delivery configurations, page 330
• Creating or modifying content delivery configurations, page 331
• Configuring the advanced properties of a content delivery configuration, page 333
• Configuring replication properties for a content delivery configuration, page 338
• Configuring extra arguments for a content delivery configuration, page 339
• Deleting content delivery configurations, page 353
• Testing content delivery configurations, page 353
• Duplicating a content delivery configuration, page 354
• Deactivating a content delivery configuration, page 354
• Publishing objects, page 355
• Content delivery configuration results, page 356
• Content delivery logs, page 357
• Effective labels, page 358

Content delivery services

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. Publication can occur on demand or automatically on a schedule.

IDS and IDSx offer the following capabilities:

• Replication of content and metadata that is published on an IDSx staging target to multiple replication targets. The replication process can occur through Content Server jobs or on demand.

• Bi-directional content delivery (publish/replicate) to a target and pulling content back to the repository. This process is known as Ingestion.
For publishing, IDSx must be installed on the computer where the repository is hosted (the source machine) and on the website host (the target machine). For replication, the IDSx target software must be installed on all the replication targets. IDSx uses accelerated data transfer technology for faster file transfer.

The *EMC Documentum Interactive Delivery Services Accelerated Installation Guide* and *EMC Documentum Interactive Delivery Services Accelerated User Guide* documentation provides additional information about Interactive Delivery Services Accelerated (IDSx).

The *EMC Documentum Interactive Delivery Services Installation Guide* and *EMC Documentum Interactive Delivery Services User Guide* documentation provides additional information about Interactive Delivery Services (IDS).

## 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 **Current** 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**.

When you access an existing content delivery configuration, the following information about the configuration displays:

**Table 91. Content delivery configuration information**

<table>
<thead>
<tr>
<th>Label</th>
<th>Information</th>
</tr>
</thead>
<tbody>
<tr>
<td>Initial Publishing Date</td>
<td>The date documents were first published using this configuration.</td>
</tr>
<tr>
<td>Refresh Date</td>
<td>The date of the last successful full refresh of the content delivery configuration.</td>
</tr>
<tr>
<td>Label</td>
<td>Information</td>
</tr>
<tr>
<td>-----------------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Last Increment Date</td>
<td>The date of the last successful incremental publish event for the content delivery configuration.</td>
</tr>
<tr>
<td>Increment Count</td>
<td>The number of successful incremental updates since the initial publish operation or last full refresh.</td>
</tr>
<tr>
<td>Publishing Status</td>
<td>Indicates whether the last publishing event succeeded or failed.</td>
</tr>
<tr>
<td>Event Number</td>
<td>Unique number generated internally for each publishing operation.</td>
</tr>
</tbody>
</table>

**Creating or modifying content delivery configurations**

Use these instructions to create content delivery configurations. You must have superuser privileges to create or modify a content delivery configuration. The user authentication is mandatory in IDSx. All fields required for publishing are on the Info tab of the Content Delivery Configuration page.

**To create or modify 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:
   - To create a content delivery configuration:
     - Select the IDS Configuration Template and then select File > Save As to access the New Content Delivery Configuration page.
     - The IDS Configuration Template stores default values that you can use to create new content delivery configurations.
     - Select File > New > Content Delivery Configuration to access the New Content Delivery Configuration page.
   - To modify an existing content delivery configuration, select the content delivery configuration to change and then select View > Properties > Info.
4. Enter content delivery configuration information on the Info tab of the New Content Delivery Configuration page, as described in Table 92, page 332. All fields on this page are required for publishing.
5. Click the Advanced tab of the New Content Delivery Configuration page and enter additional content delivery configuration information, as described in Configuring the advanced properties of a content delivery configuration, page 333.
6. Click the Replication tab of the New Content Delivery Configuration page and enter replication and transfer authentication information, as described in Configuring replication properties for a content delivery configuration, page 338.

   **Note:** The Replication tab is only available in IDSx.

7. Click Extra Arguments tab and select one or more extra arguments, as described in Configuring extra arguments for a content delivery configuration, page 339.

8. Click OK to save the content delivery configuration.

### Table 92. Content delivery properties

<table>
<thead>
<tr>
<th>Field label</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Info tab</strong></td>
<td></td>
</tr>
<tr>
<td>State</td>
<td>Select <strong>Active</strong> to indicate using this content delivery configuration is active. The default state is Active. Select <strong>Inactive</strong> to deactivate the configuration.</td>
</tr>
<tr>
<td>Configuration Name</td>
<td>Identifies the publishing configuration. The name appears in the list of existing configurations and the name of log files applying to the configuration.</td>
</tr>
<tr>
<td>Publishing Folder</td>
<td>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.</td>
</tr>
<tr>
<td>Version</td>
<td>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. If you specify a symbolic label, the case must match the label case in the repository. To allow documents with different version labels to be published, specify ANY VERSION.</td>
</tr>
<tr>
<td>Target Host Name</td>
<td>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.</td>
</tr>
</tbody>
</table>
### Configuring the advanced properties of a content delivery configuration

Use the properties described in the Advanced properties for content delivery table to configure the advanced properties of a content delivery configuration.

<table>
<thead>
<tr>
<th>Field label</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Target Port</td>
<td>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.</td>
</tr>
<tr>
<td>Target UDP Port</td>
<td>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.</td>
</tr>
<tr>
<td>Note: The Target UDP Port option is available only in IDSx.</td>
<td></td>
</tr>
<tr>
<td>Connection Type</td>
<td>Can 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.</td>
</tr>
<tr>
<td>Target Root Directory</td>
<td>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.</td>
</tr>
<tr>
<td>CAUTION: During initial publication or a full refresh, the contents of the target root directory are deleted. Ensure that you designate the correct directory as the target root directory.</td>
<td></td>
</tr>
</tbody>
</table>
Table 93. Advanced properties for content delivery

<table>
<thead>
<tr>
<th>Field label</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Property Export Settings</strong></td>
<td></td>
</tr>
<tr>
<td>Add properties as HTML Meta Tags</td>
<td>If selected, the system inserts document properties into HTML content files as META tags on the target host.</td>
</tr>
<tr>
<td></td>
<td>If this setting changes after the initial publishing event for the configuration, republish using the Full Refresh option.</td>
</tr>
<tr>
<td>Export Properties</td>
<td>If selected, the system exports a default set of properties for each published document.</td>
</tr>
<tr>
<td></td>
<td>If this setting changes after the initial publishing event for the configuration, republish using the Full Refresh option.</td>
</tr>
<tr>
<td>Include contentless properties</td>
<td>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.</td>
</tr>
<tr>
<td></td>
<td>By default, this option is not selected and is enabled only if Export Properties is also selected.</td>
</tr>
<tr>
<td>Include folder properties</td>
<td>If selected, folder properties are published to the website. This option is enabled only if Include contentless properties is also selected.</td>
</tr>
<tr>
<td>Additional Properties</td>
<td>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.</td>
</tr>
<tr>
<td></td>
<td>If this setting changes after initial publishing event for the configuration, republish using the Full Refresh option.</td>
</tr>
<tr>
<td></td>
<td>Click Select Attributes to identify additional properties to export.</td>
</tr>
<tr>
<td>Property Table Name</td>
<td>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.</td>
</tr>
<tr>
<td></td>
<td>If this setting changes after initially publishing the configuration, republish the configuration using the Full Refresh option.</td>
</tr>
</tbody>
</table>

**Content Selection Settings**
<table>
<thead>
<tr>
<th>Field label</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Formats</td>
<td>The content formats to publish. If specified, only documents with the listed formats are published. If unspecified, all formats are published.</td>
</tr>
<tr>
<td></td>
<td>If this setting changes after publishing the configuration initially, republish the configuration using the Full Refresh option.</td>
</tr>
<tr>
<td>Effective Label</td>
<td>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.</td>
</tr>
<tr>
<td></td>
<td>If this setting changes after initially publishing the configuration, you must republish the configuration using the Full Refresh option.</td>
</tr>
</tbody>
</table>

**Miscellaneous Settings**

<table>
<thead>
<tr>
<th>Field label</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Export Directory</td>
<td>The name of the local directory on the Content Server host where documents are placed after they are exported from the repository.</td>
</tr>
<tr>
<td></td>
<td>The default is a subdirectory of $DOCUMENTUM/share/temp. When executing a publishing operation, the directory $DOCUMENTUM/share/temp/web_publish is created.</td>
</tr>
<tr>
<td></td>
<td>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 Linux.</td>
</tr>
<tr>
<td>Ingest Directory</td>
<td>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.</td>
</tr>
<tr>
<td>Trace Level</td>
<td>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.</td>
</tr>
<tr>
<td>Field label</td>
<td>Value</td>
</tr>
<tr>
<td>-----------------------------</td>
<td>-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Global Publishing Enabled</td>
<td>Enables the global publishing feature of Web Publisher. Replaces the global_publishing extra argument that was added manually to the content delivery configuration in prior versions.</td>
</tr>
<tr>
<td>Website Locale</td>
<td>Web Publisher only. Replaces the global_locales 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. The drop-down list contains choices only when you are using Web Publisher and the publishing folder is configured for multilingual use. 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.</td>
</tr>
<tr>
<td>Web Server URL Prefix</td>
<td>This is the URL to the target root directory and is required if using Web Publisher. For example, if the target root directory is d:\inetpub\wwwroot\webcache and the website host is on a computer host_name, set the Web Server URL Prefix to http://host_name/webcache. <strong>Note: Web Server URL Prefix is not applicable to replication targets.</strong></td>
</tr>
<tr>
<td>Synchronization Settings</td>
<td></td>
</tr>
<tr>
<td>Transfer is to live website</td>
<td>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. If this setting changes after initial publication, republish the configuration using the Full Refresh option.</td>
</tr>
<tr>
<td>Field label</td>
<td>Value</td>
</tr>
<tr>
<td>----------------------------------------</td>
<td>------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Online Synchronization Directory</td>
<td>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. If this setting changes after you publish the configuration initially, republish the configuration using the Full Refresh option.</td>
</tr>
<tr>
<td>Pre-Synch Script on Target</td>
<td>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.</td>
</tr>
<tr>
<td>Post-Synch Script on Target</td>
<td>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.</td>
</tr>
<tr>
<td>Ingest Settings</td>
<td></td>
</tr>
<tr>
<td>Ingest</td>
<td>Select this option if you want to ingest content from the target to the repository.</td>
</tr>
<tr>
<td>Target Ingest Directory</td>
<td>Enter the directory path of the target from where the content will be ingested.</td>
</tr>
<tr>
<td>Transfer Authentication Settings</td>
<td></td>
</tr>
<tr>
<td>Enable system authentication on target</td>
<td>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.</td>
</tr>
<tr>
<td>User Name</td>
<td>Identifies the user whose account will be used by the transfer agent to connect to the target host.</td>
</tr>
<tr>
<td>Password</td>
<td>The password for the user specified in User Name.</td>
</tr>
<tr>
<td>Confirm Password</td>
<td>Enter the password again for confirmation.</td>
</tr>
<tr>
<td>Domain</td>
<td>Identifies the domain of the user specified in User Name.</td>
</tr>
</tbody>
</table>
Configuring replication properties for a content delivery configuration

Use the properties described in the content delivery replication properties table to configure replication properties for a content delivery configuration.

Table 94. Content delivery replication properties

<table>
<thead>
<tr>
<th>Field label</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Replication Target Host Settings</td>
<td>You can select one of the following states:</td>
</tr>
<tr>
<td>State</td>
<td>• Active in-transaction:Select this option if you want a replication target to participate in a transactional replication. This is the default value.</td>
</tr>
<tr>
<td></td>
<td>• Active not-in-transaction:Select this option if you want the replication target to participate in a non transactional replication.</td>
</tr>
<tr>
<td></td>
<td>• Inactive: Select this option if you want a replication target to go for system maintenance or out of commission.</td>
</tr>
<tr>
<td>Target Host Name</td>
<td>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.</td>
</tr>
<tr>
<td>Target Port</td>
<td>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.</td>
</tr>
<tr>
<td>Target UDP Port</td>
<td>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.</td>
</tr>
<tr>
<td>Connection Type</td>
<td>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.</td>
</tr>
</tbody>
</table>
## Field label | Value
---|---
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.

### Transfer Authentication Settings

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.

## Configuring extra arguments for a content delivery configuration

Use the following instructions and the properties described in the extra arguments table to configure extra arguments for a content delivery configuration.

**To create or modify extra arguments:**

1. On the 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.
   
   You can use the **Move Up** or **Move Down** buttons to rearrange the order of the extra arguments.
   
   To delete an argument, select an extra argument on the right side and then click **Remove**.
4. Click OK.

Table 95. Extra arguments

<table>
<thead>
<tr>
<th>Key</th>
<th>Description</th>
<th>Default Value(s)</th>
</tr>
</thead>
<tbody>
<tr>
<td>use_docbase_formats</td>
<td>Determines whether the default file format extensions set in the repository are used when files are published.</td>
<td>TRUE</td>
</tr>
<tr>
<td></td>
<td>FALSE overrides the default file format extensions set in the repository.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>TRUE or no setting uses the extensions set in the repository format objects.</td>
<td></td>
</tr>
<tr>
<td>use_text_file_extensions</td>
<td>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.</td>
<td>FALSE</td>
</tr>
<tr>
<td>agent_connection_timeout</td>
<td>The timeout interval in seconds for the IDS publish method’s connection to the target host. For example, to wait 90 seconds:</td>
<td>120</td>
</tr>
<tr>
<td></td>
<td>agent_connection_timeout=90</td>
<td></td>
</tr>
<tr>
<td></td>
<td>If the publishing operation takes longer, Documentum Administrator displays an error message and the publishing log files record that the publishing operation failed.</td>
<td></td>
</tr>
<tr>
<td>connect_thread_timeout</td>
<td>The timeout interval in seconds for the end-to-end tester’s connection to the target host. For example, to wait 90 seconds:</td>
<td>30</td>
</tr>
<tr>
<td></td>
<td>connect_thread_timeout=90</td>
<td></td>
</tr>
<tr>
<td>Key</td>
<td>Description</td>
<td>Default Value(s)</td>
</tr>
<tr>
<td>---------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
<td>------------------</td>
</tr>
<tr>
<td>lock_sleep_interval</td>
<td>The number of seconds for which IDS waits for a webc lock object to be unlocked. For example, to wait 90 seconds: <code>lock_sleep_interval=90</code></td>
<td>10</td>
</tr>
<tr>
<td>lock_retry_count</td>
<td>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.</td>
<td>30</td>
</tr>
<tr>
<td>disable_dctm_tag</td>
<td>Whether you want the Documentum META tag to appear when you use META tag merging.</td>
<td>TRUE</td>
</tr>
<tr>
<td>trace_passwords</td>
<td>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.</td>
<td>FALSE</td>
</tr>
<tr>
<td>error_threshold</td>
<td>The number of errors allowable on the source side during a single full-refresh, incremental, or force-refresh publishing operation.</td>
<td>0</td>
</tr>
<tr>
<td>maxCached_ssl_sockets</td>
<td>The number of cached SSL sockets between source and all targets that are retained for reuse. Does not restrict the maximum number of SSL sockets that can be open at one time. Used only in the scs_admin_config object in the IDS Administration sub-node.</td>
<td>30</td>
</tr>
<tr>
<td>Key</td>
<td>Description</td>
<td>Default Value(s)</td>
</tr>
<tr>
<td>-----------------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
<td>------------------</td>
</tr>
<tr>
<td>publish_contentless_documents</td>
<td>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.</td>
<td>FALSE</td>
</tr>
<tr>
<td>publish_folder_properties</td>
<td>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.</td>
<td>FALSE</td>
</tr>
<tr>
<td>compression</td>
<td>Whether file compression is enabled. TRUE causes files to be compressed. FALSE disables file compression.</td>
<td>TRUE</td>
</tr>
<tr>
<td>min_size_worth_compressing</td>
<td>The threshold in bytes beneath which compression of a particular file does not yield performance gains</td>
<td>5000</td>
</tr>
<tr>
<td>max_entries_per_zipfile</td>
<td>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.</td>
<td>128</td>
</tr>
<tr>
<td>extensions_to_compress</td>
<td>The file types to compress, by file extension.</td>
<td>html, jhtml, shtml, phtml, xhtml, htm, jht, sht, asp, jsp, xml, css, txt</td>
</tr>
<tr>
<td>publish_source_version_labels</td>
<td>When set to TRUE, all values of the r_version_label attribute are published to the repeating attribute table.</td>
<td>FALSE</td>
</tr>
<tr>
<td>Key</td>
<td>Description</td>
<td>Default Value(s)</td>
</tr>
<tr>
<td>----------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
<td>------------------</td>
</tr>
<tr>
<td>mssql_store_varchar</td>
<td>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. When set to true, you cannot publish multibyte data.</td>
<td>FALSE</td>
</tr>
<tr>
<td>store_log</td>
<td>Whether to store log files in the repository. Valid values are:</td>
<td>TRUE</td>
</tr>
<tr>
<td></td>
<td>• TRUE: The logs are stored in the repository.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• FALSE: The logs are not stored in the repository.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>The log is not stored in the repository for a single-item publishing operation when method_trace_level is set to 0.</td>
<td></td>
</tr>
<tr>
<td>store_log_file</td>
<td>Determines whether publishing logs are deleted or retained on the source host. If the key is set to TRUE, publishing logs are preserved. If the key is set to FALSE, the trace level is less than 10; if the publishing operation succeeds, the log files are deleted.</td>
<td></td>
</tr>
<tr>
<td>method_trace_level</td>
<td>The level of tracing output. 0 is the lowest level of tracing and 10 is the highest level of tracing.</td>
<td>0</td>
</tr>
<tr>
<td></td>
<td><strong>Note:</strong> To get LDAPSync debug information, use method_trace_level 8. To get verbose debug information, use method_trace_level 10.</td>
<td></td>
</tr>
<tr>
<td>export_threshold_count</td>
<td>Indicates the number of items the export operation exports at one time.</td>
<td>100</td>
</tr>
<tr>
<td>Key</td>
<td>Description</td>
<td>Default Value(s)</td>
</tr>
<tr>
<td>----------------------------</td>
<td>-----------------------------------------------------------------------------</td>
<td>------------------</td>
</tr>
<tr>
<td>use_format_extensions</td>
<td>Use with format key to check for valid format extensions.</td>
<td>FALSE</td>
</tr>
<tr>
<td></td>
<td>If use_format_extensions is set to FALSE, files are published with the format extensions defined in the repository for the format.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>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.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>If use_format_extensions is set to TRUE and a particular extension is not defined as valid for a particular format, files of that format with that extension are published with the format extensions defined in the repository for the format.</td>
<td></td>
</tr>
<tr>
<td>format</td>
<td>Use with use_format_extensions key. Takes the format:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>format.format_name=semicolon-separated_extensions</td>
<td></td>
</tr>
<tr>
<td>force_serialized</td>
<td>When set to TRUE, single-item publishes are performed serially rather than in parallel.</td>
<td>FALSE</td>
</tr>
<tr>
<td>source_attrs_only</td>
<td>By default, on each publish IDS creates a properties.xml file, which contains all the attributes of the objects published.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>If source_attrs_only is set, IDS writes only the default attributes and any additional attributes that are published to the XML file.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• r_object_id</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• r_modified_date</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• object_name</td>
<td></td>
</tr>
<tr>
<td>Key</td>
<td>Description</td>
<td>Default Value(s)</td>
</tr>
<tr>
<td>------------------------------</td>
<td>-----------------------------------------------------------------------------</td>
<td>---------------------------</td>
</tr>
<tr>
<td>• i_chronicle_id</td>
<td></td>
<td></td>
</tr>
<tr>
<td>• r_version_label</td>
<td></td>
<td></td>
</tr>
<tr>
<td>• content_id</td>
<td></td>
<td></td>
</tr>
<tr>
<td>• i_full_format</td>
<td></td>
<td></td>
</tr>
<tr>
<td>• r_folder_path</td>
<td></td>
<td></td>
</tr>
<tr>
<td>additional_metatag_file_exts</td>
<td>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:</td>
<td>No default value.</td>
</tr>
<tr>
<td></td>
<td>additional_metatag_extensions= asp;jsp;jht;sht</td>
<td></td>
</tr>
<tr>
<td>export_relations</td>
<td>When set to TRUE and attributes are published, relation objects (dm_relation objects) are published to a database table on the target.</td>
<td>FALSE</td>
</tr>
<tr>
<td>clean_repeating_table_no_attrs</td>
<td>Deprecated.</td>
<td></td>
</tr>
<tr>
<td>export_media_properties</td>
<td>When set to true, attributes of the dmr_content object and dm_format object are exported and published to the target.</td>
<td>FALSE</td>
</tr>
<tr>
<td>additional_media_properties</td>
<td>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:</td>
<td>FALSE</td>
</tr>
<tr>
<td></td>
<td>additional_media_properties=type1.attribute1;type2.attribute2</td>
<td></td>
</tr>
<tr>
<td></td>
<td>For example:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>additional_media_properties=dmr_content.x_range;dmr_content.z_range</td>
<td></td>
</tr>
<tr>
<td>Key</td>
<td>Description</td>
<td>Default Value(s)</td>
</tr>
<tr>
<td>----------------------------</td>
<td>-----------------------------------------------------------------------------------------------------------------------------------------------</td>
<td>------------------</td>
</tr>
<tr>
<td>exclude_folders</td>
<td>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:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>exclude_folders=/acme.com/images;/acme.com/subdir</td>
<td></td>
</tr>
<tr>
<td>pre_webroot_switch_script</td>
<td>A script to be run before online synchronization takes place. &quot;Scripts run before or after the Webroot Switch” in the EMC Documentum Interactive Delivery Services User Guide, provides the detailed information.</td>
<td></td>
</tr>
<tr>
<td>post_webroot_switch_script</td>
<td>A script to be run after online synchronization takes place. &quot;Scripts run before or after the Webroot Switch” in the EMC Documentum Interactive Delivery Services User Guide, provides the detailed information.</td>
<td></td>
</tr>
<tr>
<td>full_refresh_backup</td>
<td>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.</td>
<td>FALSE</td>
</tr>
<tr>
<td>exclude_formats</td>
<td>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:</td>
<td>Not set</td>
</tr>
<tr>
<td></td>
<td>exclude_formats=xml;wml</td>
<td></td>
</tr>
<tr>
<td>Key</td>
<td>Description</td>
<td>Default Value(s)</td>
</tr>
<tr>
<td>----------------------------</td>
<td>-----------------------------------------------------------------------------</td>
<td>-----------------------------------------</td>
</tr>
<tr>
<td>check_valid_filename</td>
<td>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. 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.</td>
<td>TRUE (Windows only); FALSE for all other O/S</td>
</tr>
<tr>
<td>filename_replace_char</td>
<td>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: filename_replace_char=0</td>
<td>_ (underscore)</td>
</tr>
<tr>
<td>sync_on_zero_updates</td>
<td>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.</td>
<td>FALSE</td>
</tr>
<tr>
<td>transform_type</td>
<td>Used with Web Publisher Page Builder only. Determines whether links in HTML pages are resolved at publication time to absolute or relative paths. Valid values are absolute and relative.</td>
<td>absolute</td>
</tr>
<tr>
<td>recovery_publish_retry_count</td>
<td>Controls the number of times IDSx tries to recover from a failed incremental publishing operation. The value is an integer that represents the number of times IDSx retries the publishing operation.</td>
<td></td>
</tr>
<tr>
<td>Key</td>
<td>Description</td>
<td>Default Value(s)</td>
</tr>
<tr>
<td>----------------------------</td>
<td>------------------------------------------------------------------------------</td>
<td>------------------</td>
</tr>
<tr>
<td>set_tcp_delay</td>
<td>Determines TCP protocol behavior. With the default setting of FALSE, packets are sent to the target as soon as they are written on the source side; IDSx does not wait until the sockets buffer is filled or there is a timeout. For debugging purposes, this parameter can be set to TRUE. The setting must match the same key in agent.ini.</td>
<td>FALSE</td>
</tr>
</tbody>
</table>
| ingest_workflow            | Used with Content Delivery web service only. Specifies a custom workflow to be used with the ingest operation. The *EMC Documentum Enterprise Content Services Reference Guide* provides detail 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.  
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. | 22               |
| 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)

<table>
<thead>
<tr>
<th>Key</th>
<th>Description</th>
<th>Default Value(s)</th>
</tr>
</thead>
<tbody>
<tr>
<td>wan_acceleration_policy</td>
<td>This parameter defines the policy used for accelerated data transfer.</td>
<td>A</td>
</tr>
<tr>
<td></td>
<td>• 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.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• 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.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• 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.</td>
<td></td>
</tr>
<tr>
<td>min_file_transfer_rate</td>
<td>This is the minimum file transfer rate</td>
<td>0 Mbps</td>
</tr>
<tr>
<td>max_file_transfer_rate</td>
<td>This is the maximum file transfer rate</td>
<td>1000 Mbps</td>
</tr>
<tr>
<td>wan_acceleration_log_details</td>
<td>The file transfer process status are captured in the content delivery log files</td>
<td>FALSE</td>
</tr>
<tr>
<td>Key</td>
<td>Description</td>
<td>Default Value(s)</td>
</tr>
<tr>
<td>------------------------------------------</td>
<td>-----------------------------------------------------------------------------</td>
<td>------------------</td>
</tr>
<tr>
<td>wan_acceleration_file_checksum</td>
<td>This parameter is used to resume file transfer when there is a failure.</td>
<td>OFF</td>
</tr>
<tr>
<td></td>
<td>• 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.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• FULL_CHECKSUM: When set to this value, checks for the checksum of both files. If it matches, then transfer does not take place.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• SPARSE_CHECKSUM: When set to this value, checks for the sparse checksum of both files. If it matches, then transfer does not take place.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• OFF: When set to this value, the file gets replaced.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>When set to OFF, the rate of file transfer is high.</td>
<td></td>
</tr>
<tr>
<td>decision_commitrollback</td>
<td>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:</td>
<td>NA</td>
</tr>
<tr>
<td></td>
<td>decision_commitrollback 6</td>
<td></td>
</tr>
<tr>
<td></td>
<td>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.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>If the number_of_failures value is greater than the decision_commitrollback value, a rollback is initiated on the replication targets.</td>
<td></td>
</tr>
<tr>
<td>Key</td>
<td>Description</td>
<td>Default Value(s)</td>
</tr>
<tr>
<td>------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
<td>------------------</td>
</tr>
<tr>
<td>tc_file_count</td>
<td>The transaction capability is based on tc_file_size and tc_file_count. When the number of files replicated exceeds tc_file_count, transaction capability feature is disabled.</td>
<td>500</td>
</tr>
<tr>
<td>tc_file_size</td>
<td>The transaction capability is based on tc_file_size and tc_file_count. When the size of the files replicated exceeds tc_file_size, transaction capability feature is disabled. The units is specified in MB.</td>
<td>100 MB</td>
</tr>
<tr>
<td>use_replication_time</td>
<td>Use this extra argument to ensure that after replication is complete, all the replication targets will display the same time stamp as when the replication was triggered.</td>
<td>TRUE</td>
</tr>
<tr>
<td>use_repository_time</td>
<td>Use this extra argument to ensure that after replication is complete, all the replication targets will display the same time stamp as when the content was last modified in the docbase (r_modified_date when the file was replicated).</td>
<td>TRUE</td>
</tr>
<tr>
<td>Key</td>
<td>Description</td>
<td>Default Value(s)</td>
</tr>
<tr>
<td>-----------------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
<td>------------------</td>
</tr>
<tr>
<td>lock_exitifbusy_flag</td>
<td>During publishing or replication operations, IDSx locks a configuration using a webc lock object, so that only one publishing or replication operation can take place at a time for that configuration. If you want IDSx to exit rather than retry when the publishing configuration is locked, set the lock_exitifbusy_flag argument to TRUE.</td>
<td>TRUE</td>
</tr>
<tr>
<td>auto_replication</td>
<td>Replication can be invoked automatically after a publishing operation by setting the extra argument auto_replication to TRUE in Documentum Administrator. Note: Concurrent single item publishing at the same time as auto replication causes a considerable load on the staging target. Hence, set the extra argument lock_exitifbusy_flag along with auto_replication to TRUE. The subsequent replication process will consider all the published batches that were left unused during the creation of the previous replication batch.</td>
<td>TRUE</td>
</tr>
<tr>
<td>full_refresh_transactional_replication</td>
<td>The replication process can start a transactional replication, even when the replication batch being replicated contains a full refresh publish. Replication Manager can be enhanced to start a transactional replication setting the extra arguments, full_refresh_transactional_replication and full_refresh_backup, to TRUE for full refresh publish.</td>
<td>FALSE</td>
</tr>
<tr>
<td>post_replication_script_on_staging_target</td>
<td>Use this script to perform any arbitrary action on the staging target after replication</td>
<td>No default value.</td>
</tr>
</tbody>
</table>
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 354 provides instructions on how to inactivate 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
   ```plaintext
   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.
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.

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 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 options 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. The EMC Documentum Interactive Delivery Services User Guide and EMC Documentum Interactive Delivery Services Accelerated User Guide provides 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 357
- Deleting content delivery logs, page 357

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.
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 aExpiration_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 aExpiration_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 96. Using effective labels

<table>
<thead>
<tr>
<th>a_effective_label</th>
<th>a_effective_date</th>
<th>aExpiration_date</th>
</tr>
</thead>
<tbody>
<tr>
<td>DRAFT</td>
<td>03/05/08</td>
<td>03/15/08</td>
</tr>
<tr>
<td>REVIEW</td>
<td>03/16/08</td>
<td>03/26/08</td>
</tr>
<tr>
<td>COMMENT</td>
<td>03/27/08</td>
<td>04/10/08</td>
</tr>
<tr>
<td>APPROVED</td>
<td>04/10/08</td>
<td>04/10/09</td>
</tr>
</tbody>
</table>

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 13

Indexing Management

This chapter contains the following topics:

- Indexing, page 359
- Index agents and xPlore, page 359
- Starting and stopping index agents, page 360
- Disabling index agents, page 360
- Enabling index agents, page 361
- Verifying indexing actions, page 361
- Viewing or modifying index agent properties, page 361
- Managing index queue items, page 362

Indexing

A full-text index is an index on the properties and content files associated with documents or other SysObjects or SysObject subtypes. Full-text indexing enables the rapid searching and retrieval of 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 Documentum xPlore creates indexes and responds to queries from Content Server. The EMC Documentum xPlore Deployment Guide provides information on installing the index agent and xPlore.

You must have system administrator or superuser privileges to start, stop, or disable index agents, start or stop xPlore, and manage queue items. The EMC Documentum xPlore Administration Guide provides information on editing the properties of the index agent configuration object and other full-text configuration objects.

Index agents and xPlore

The Index Agents and Index Servers list page shows the index agent and index queue associated with the repository.
The index agent exports documents from a repository and prepares them for indexing. A particular index agent runs against only one repository. xPlore creates full-text indexes and responds to full-text queries from Content Server.

## Starting and stopping index agents

Use these instructions to stop a running index agent or start an index agent that is stopped.

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 before starting it. Enabling index agents, page 361 provides information on enabling a disabled index agent. 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.

**Note:** If the Content Server is in a *projected to dormant* state, then starting or stopping the index agent works correctly. However, if the Content Server is in a *dormant* state, then starting or stopping the index agent using Documentum Administrator does not work correctly. The status of the index agent appears as **Not Responding**. The index agent logs contain the following error: `[DM_INDEX_AGENT_UNEXPECTED_DFC_EXCEPTION] Unexpected DfException: context: Init Connector cause: [DM_SESSION_E_OP_DISALLOWED_IN_STATE_UNLESS_ENABLED]error: "The operation (Opening a new transaction) is disallowed when the server is in Dormant state unless enabled by Data Center Managers on their sessions."

## 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 361.
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, 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.

## 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 active-active configuration, with multiple index agents and xPlore installations, each index agent/xPlore federation 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.

If the indexing system is in a high-availability active-active 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.

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 xPlore federation

- **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. The *EMC Documentum xPlore Administration Guide* provides instructions about resubmitting objects for indexing.

**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.
This chapter contains the following topics:

• Content Transformation Services, page 367
• Changing the CTS user, page 367
• Configuring a CTS instance, page 368
• Viewing a CTS log file, page 371
• Viewing details of a CTS instance, page 372
• Controlling your CTS instance, page 372
• CTS reporting, page 374

Content Transformation Services

Content Transformation Services version 7.2 encapsulates the functionality of all transformation components (Document Transformation Services, Advanced Document Transformation Services, Media Transformation Services and Audio/Video Transformation Services) and requires just one installation, rather than multiple installation processes for multiple Content Transformation Services components. Content Transformation Services (CTS) versions prior to version 7.0 include Document Transformation Services, Advanced Document Transformation Services, Audio/Video Transformation Services, Media Transformation Services and a number of add-on components.

A repository can be polled by multiple CTS instances. All CTS instances polling the repository are displayed in the Content Transformation Services node in Documentum Administrator.

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 > Content Transformation Services 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 > Configure > 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 368
• Changing the logging level, page 369
• Changing the System Operator, page 369
• Changing the notification setting, page 370
• Changing the maximum number of queue items, page 370
• Changing the queue item expiry, page 371

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 > Content Transformation Services 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 > Service.
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 > Content Transformation Services** 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 > Service**.
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 > Content Transformation Services** 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 > Service.
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 > Content Transformation Services 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 > Service.
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 > Content Transformation Services 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 > Service.
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 > Content Transformation Services 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 > Service.
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 369).

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 > Content Transformation Services 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**: The name of the product.
- **Version**: The version number of the product.
- **Hostname**: The name of the host machine for the 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 > Content Transformation Services 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

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 372
- Starting the CTS service, page 373
- Refreshing the CTS service, page 373

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 > Content Transformation Services 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.
   • 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 > Info.
     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 refreshed date and time is shown when the page is reloaded.

To start a CTS instance:
1. Connect to the repository where the CTS instance is located.
2. Click the Administration > Content Transformation Services 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.
   • 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 > Content Transformation Services 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.
   • Click Tools > Content Transformation Services > Refresh.
   OR
   • 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.
5. 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 374
• Viewing archived CTS reporting data, page 375

**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 > Content Transformation Services 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 15

Content Intelligence Services

This chapter contains the following topics:

• Content Intelligence Services in Documentum applications, page 377
• Classic categorization in Webtop, page 378
• Content Intelligence Services in xCP deployments, page 378
• Configuring Content Intelligence Services in Documentum Administrator, page 379
• Building taxonomies for classic categorization, page 383
• Selecting and submitting the documents to analyze, page 405
• Managing analysis results, page 411

Content Intelligence Services in Documentum applications

Use Content Intelligence Services (CIS) to analyze the textual content of documents and know what the documents are about without having to read them.

By default, CIS analyzes the content of the documents, including the values of the file properties. You can change the default behavior and have CIS analyze the values of the Documentum object attributes in addition to, or instead of, the content of the documents.

CIS performs several types of analysis:

• **Categorization**: By detecting predefined keywords in the document content, the categorization identifies the category to which a document belongs. Categories for a subject area are organized in a structure called a taxonomy. Categorization enables you to organize content in a logical and consistent way.

• **Entity detection**: It relies on Natural Language Processing (NLP). Named entities are detected by performing a semantic analysis of their context. If there is too little context, or if the context is unclear, the detection can seem to be incomplete. You can use entity detection to find named entities such as people names or company names in documents.

• **Pattern detection**: Some pieces of information always have the same form. Use the pattern detection to retrieve this information when it is disseminated in text. For example, email addresses, because they comply with a standard, can be extracted using pattern detection. Pattern detection retrieves all pieces of information that match the pattern.
Related topics:
- Classic categorization in Webtop, page 378
- Content Intelligence Services in xCP deployments, page 378

Classic categorization in Webtop

Like in the previous Documentum versions, you can perform categorization for a WDK-based application. This mode of categorization is referred to as classic categorization.

Use classic categorization to reach the following goals:

- Enable users to see the documents in the taxonomy hierarchy. 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 folder link between the document and the category.
- Update an attribute with the category name. When a document is categorized, CIS writes the names of assigned categories in the attribute of the document.

The configuration of classic categorization is done using Documentum Administrator and at the CIS server level.

Classic categorization can be:
- **Automatic**: CIS server analyzes documents and assigns them to appropriate categories.
- **Manual**: a person assigns documents to categories.
- **Semi-automatic**: Documentum Administrator enables you to review the results of either type of categorization, and to adjust them manually if necessary. For documents that CIS server cannot definitively assign to particular categories, category owners approve or reject the candidate documents in Documentum Administrator.

Related topic: Setting up Content Intelligence Services for classic categorization, page 379

Content Intelligence Services in xCP deployments

Content Intelligence Services is also available in xCP deployments, starting with xCP 2.0. To use CIS in xCP deployments, define discovered metadata attributes in content models. Discovered metadata is metadata found by content analytics. The full list of out-of-the-box discovered metadata attributes is available in xCP Designer documentation.

Entity detection and pattern detection are available in xCP applications and when accessing analysis results with the Annotations API.

Categorization is also available in xCP applications but the taxonomies used for categorization are not available in the Content Intelligence node in Documentum Administrator.

For xCP deployments, the configuration is done using xCP Designer. Additional configuration is possible using Documentum Administrator. Use Documentum Administrator for actions related to document sets such as modifying the document set configuration or clearing the analysis results for a document set.
The following actions are not available for categorization in xCP deployments:

- Testing taxonomies. As a consequence, it is not possible to define a second CIS server to test taxonomies.
- Assigning documents manually or submitting documents individually for categorization.
- Bringing taxonomies online or offline. As soon as a content model is configured to use categorization and discovered metadata attributes are exposed in a page, the results of categorization are visible to end users.
- Exposing the taxonomy hierarchy. It is possible to display the path corresponding to the position of the category in the hierarchy but not to render the tree structure itself. In some cases, only a level of the hierarchy is displayed.

Related topics:

- Document sets, page 405
- Clearing analysis results for a document set, page 415

Configuring Content Intelligence Services in Documentum Administrator

This section contains the following topics:

- Setting up Content Intelligence Services for classic categorization, page 379
- Enabling Content Intelligence Services, page 380
- Defining Content Intelligence Services configuration, page 381
- Data synchronization between the repository and CIS server, page 382
- Missing Content Intelligence node, page 382

Setting up Content Intelligence Services for classic categorization

Before you can use CIS for classic categorization, install and start the CIS server. The *EMC Documentum Content Intelligence Services Installation Guide* provides information about installing and starting the CIS server.

After you have installed and started the CIS server, you can configure CIS using Documentum Administrator. Setting up CIS includes the following tasks:

- Configuring the repository for Content Intelligence Services.
- Designing and creating taxonomies.
- Synchronizing the taxonomies with CIS server.
- Identifying a set of test documents and checking them into a folder in the repository.
The set of documents should include representatives of the various types of documents you are processing with Content Intelligence Services. The documents help to test and fine-tune the category definitions.

- Creating a document set that selects the test documents.
- Testing the document set and review the resulting categorizations.
- Adjusting the category definitions as necessary to refine the results.
- Synchronizing taxonomy in production mode, and run the document set in production mode.
- Bringing the taxonomies online.

**Related topics:**
- Classic categorization in Webtop, page 378
- Defining Content Intelligence Services configuration, page 381

## Enabling Content Intelligence Services

Before you can use Content Intelligence Services, you must activate the CIS-related objects in the repository to which you want to apply CIS processing.

The repository is automatically enabled for CIS processing during xCP deployment phase or when installing Content Intelligence Services.

**Note:** You must be logged in as a user with superuser privileges to enable CIS processing. If you do not have sufficient privileges, 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.
   
   If the Content Intelligence node is not visible, verify if CIS DAR is correctly installed.

2. Click the Enable repository for Content Intelligence link.

   The Enable Repository for Content Intelligence page appears.

   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.

   The default path for the Content Intelligence administrative information is /System/Application/CI.

   These two locations cannot be modified.

3. 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:

   192.168.1.250:8079

   Default port number is **8079**.
You can define the host names using an IPv6 addresses. When using an IPv6 address, with or without a specific port number, enclose it with 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. 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 servers need be running when you enable the repository.

4. 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.

5. Click OK.

6. Define Content Intelligence Services configuration.

**Related topics:**

- Missing Content Intelligence node, page 382
- Test processing and production processing, page 412
- Defining Content Intelligence Services configuration, page 381

---

**Defining Content Intelligence Services configuration**

The Configuration for Content Intelligence page enables you to define how CIS records category assignments as well as the host names for the CIS servers that process documents from this repository.

You must be a member of the ci_taxonomy_manager_role to configure CIS.

**To define 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 port numbers of the CIS production and test servers. The specified CIS servers need be running when you configure the repository.

4. Select **Link assigned documents into category folders** to enable end users to view documents by browsing the category folders.

   **Note:** Selecting this option affects system performance during document processing and classification. Do not select it unless you need the functionality it provides.

   This option is not applicable in xCP deployments.

5. Select **Update document attributes with category assignments** to add the category names to the specified document attribute, as defined in the category class. This option is not applicable in xCP deployments.
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.

Related topics:
- Test processing and production processing, page 412
- Defining category classes, page 392

Data synchronization between the repository and CIS server

CIS server uses two types of resources that are defined in the repository: the taxonomies and the document sets. Each time a taxonomy or a document set is created or modified, you must make it available to CIS server so that CIS server can use the new or updated definitions to analyze documents. This process is called synchronization. Updates are not reflected in automatic processing until you synchronize the object definitions.

For classic categorization, you can select to synchronize in test mode or in production mode. If you synchronize a document set in Test mode, make sure that the specified taxonomy was synchronized in Test mode as well.

Note: If any of the categories in a taxonomy include links to categories in other taxonomies, all related taxonomies must be synchronized to avoid possible errors.

Related topics:
- Test processing and production processing, page 412
- Synchronizing taxonomies with CIS server, page 400
- Synchronizing a document set, page 409

Missing Content Intelligence node

If the Content Intelligence node is not visible, verify if CIS DAR is installed in the repository. Navigate to the Administration page > System information page > Repository section. If it indicates: Content Intelligence: CIS DAR not found in the repository, then install CIS DAR as described in the following procedure.
To deploy CIS DAR on the repository:

1. Depending on your use of the categorization functionality, proceed with one of the following options:
   - You use CIS server to categorize content: in this case, it is likely that the version of Documentum Administrator is more recent than the version of the CIS server. In this case, we recommend that you upgrade CIS to the same version as Documentum Administrator.
   - You classify manually, without CIS server.
     1. In this case, download the Content Intelligence Services archive file from the Documentum download center, for the same version as your Documentum Administrator.
     2. Unzip the archive file and navigate to the DAR folder.
     3. Deploy the module cis_artifact.dar according to Documentum guidelines for module deployment in Documentum Composer documentation.

Building taxonomies for classic categorization

This section contains the following topics:

- Taxonomies, page 384
- Category classes, page 385
- Categories, page 385
- Taxonomy manager, page 386
- Category owner, page 386
- Viewing taxonomies and categories, page 386
- Providing evidence, page 387
- Confidence values and score thresholds, page 388
- Category and taxonomy rules, page 389
- Evidence terms, page 390
- Using stemming on evidence terms, page 390
- Language detection for stemming, page 391
- Reusing category evidence, page 392
- Defining category classes, page 392
- Defining taxonomies, page 394
- Defining categories, page 395
- Defining property rules, page 397
- Defining evidence terms, page 399
- Synchronizing taxonomies with CIS server, page 400
- Making taxonomies available, page 401
Taxonomies

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.

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. The structure of a taxonomy determines the navigation path that users follow to locate documents in the category.

Content Intelligence Services also uses the term taxonomy to refer to the Documentum object that serves as the root level of the hierarchy.

Taxonomies consist of three types of Documentum objects:

- **Taxonomies**: Represent the root of a hierarchical tree of categories. The taxonomy definition sets default values for its categories and can include property conditions that documents must meet to be categorized. No documents are assigned directly to the root of the taxonomy.

- **Categories**: Are the headings under which documents are categorized. The definition of a category includes the evidence that CIS server looks for in document content to determine whether it belongs to the category.

- **Category classes**: Define the default behavior of categories. Every category is assigned to a class.

When you create a taxonomy, it is offline by default. Offline taxonomies are available for design and test, but are not available for end users to see. To make the taxonomy available to end users, you bring it online. When you bring it online, the taxonomy, its categories, and categorized documents appear to users under the Categories node in Documentum Administrator and in Webtop.

When you create or modify a taxonomy in the repository, synchronize it to make it available to CIS server.

In addition to building taxonomies using Documentum Administrator, you can import taxonomies in taxonomy exchange format (TEF). The EMC Documentum Content Intelligence Services Administration Guide provides more information about importing taxonomies.
Category classes

The properties of a category class determine the default behavior of categories belonging to the class. Categories can override the default settings. If you are using the **Assign as Attributes** option to write category assignments into document 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. Create additional category classes to assign category information to a different attribute or use different rules for generating category evidence.

Before creating a taxonomy, pay attention to the category class definition, in particular when you want to implement some inheritance. For example, to have documents matching a category only if they match the parent category, add a category link to the parent, with weight "Required", as default category evidence.

Before deleting a category class, reassign all categories to use another category class.

Related topics:
- Categories, page 385
- Defining category classes, page 392

Categories

Categories are the headings under which documents are categorized. Depending on their definition, categories can be exclusive and as simple as Confidential, Internal, Public. Categories can also be cumulative and documents can match an unlimited number of categories.

The taxonomy in which a category is created determines the following default settings:
- The default category class.
- The default on-target and candidate threshold values.

The category class selected for a category determines the following default settings:
- CIS treats the category name as an evidence term for the category.
- Set the default rules for using evidence from child or parent categories.

This configuration can be overridden in the category definition.

Related topics:
- Taxonomies, page 384
- Defining categories, page 395
Taxonomy manager

There are two roles related to Content Intelligence Services: the taxonomy manager and the category owner.

The taxonomy manager role (ci_taxonomy_manager_role) can perform the following actions:

• Create taxonomies and add categories only to their own taxonomies.
• Edit or delete the categories they have created. The owner of a category is the taxonomy manager who created it.
• Import taxonomies. If the owner is not specified during the import of a taxonomy, the CIS user defined for the repository becomes the owner of the taxonomy and its categories.
• Configure the document sets to define which documents to process and when.
• Test taxonomies and bring them online when they are ready.
• You can change the owner of a taxonomy or category. However, as for any Documentum object, the change must be done for each object (taxonomy or category). Edit the owner of the object and set it to ci_taxonomy_manager_role.

Related topics:
• Taxonomies, page 384
• Setting permissions for Content Intelligence, page 401

Category owner

The taxonomy manager selects the category owners during the category configuration. Based on their expertise, the category owners are responsible for reviewing categorized documents.

The category owner role (ci_category_owner_role) can perform the following actions:

• Approve or reject documents pending approval.
• Assign documents manually.
• Clearing analysis results.

Related topics:
• Categories, page 385
• Setting permissions for Content Intelligence, page 401

Viewing taxonomies and categories

The categories defined for classic categorization are available in several views in Documentum Administrator. The categories used in an xCP deployment are not visible in these views.

The following table describes the different views and when to use them.
Table 97. Views for categories in Documentum Administrator

<table>
<thead>
<tr>
<th>View</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Administration &gt; Content Intelligence &gt; My</td>
<td>Displays all categories at the same level as a flat list.</td>
</tr>
<tr>
<td>Categories</td>
<td>This view provides direct access to the categories for which you are the</td>
</tr>
<tr>
<td></td>
<td>owner so that you can review documents. You can view all documents</td>
</tr>
<tr>
<td></td>
<td>assigned to the categories you own, or only documents pending approval.</td>
</tr>
<tr>
<td>Administration &gt; Content Intelligence &gt; Taxonomies</td>
<td>Displays categories in their proper hierarchical position.</td>
</tr>
<tr>
<td></td>
<td>This view is the configuration and administration view for taxonomies and</td>
</tr>
<tr>
<td></td>
<td>categories. Use this view to create and configure categories.</td>
</tr>
<tr>
<td>Categories cabinet</td>
<td>Displays the hierarchy of categories and the documents assigned to these</td>
</tr>
<tr>
<td></td>
<td>categories. This view is the end user view of the categories.</td>
</tr>
</tbody>
</table>

Related topics:
- Taxonomies, page 384
- Categories, page 385

Providing evidence

The categorization quality relies on the category definitions. The more accurate the definition, the better the categorization results. To define efficient categories, you can act on several aspects:

- You can use keywords, that is, evidence terms and their respective confidence value. Evidence terms can be simple terms or phrases, for which you choose to apply a stemming analysis or keep the phrase order.

  A new category can have one simple term already defined: the name of the category. The category name can appear as text or as the keyword @implied. The category name or @implied appears when the category class for this category has the Generate evidence from category name option.

- You can define patterns using regular expressions to match specific terms such as phone numbers, social security numbers and so on. The EMC Documentum Content Intelligence Services Administration Guide provides the detailed procedure for defining patterns.

- You can set property rules that allow you to define category assignments according to the values of the repository attributes.

- You can use evidence from other categories by setting category links.

When you have created a taxonomy and provided evidence terms for each category, test how well the category definitions guide CIS server in categorizing documents.

Submit some test documents to the CIS server. If the CIS server does not assign some documents to the categories you expect it to, consider revising the category thresholds or the evidence associated with the categories.
If documents appear in a category they should not, it means that the evidence for that category is too broad: consider adding additional terms or increasing the confidence thresholds. If documents do not appear in the category they should, the evidence is too restrictive: consider lowering 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.

Related topics:
• Confidence values and score thresholds, page 388
• Using stemming on evidence terms, page 390
• Category and taxonomy rules, page 389
• Evidence terms, page 390
• Defining category classes, page 392
• Reusing category evidence, page 392

Confidence values and score thresholds

Each category definition lists the words and phrases that serve as evidence that a document belongs to the category. These words and phrases are called evidence terms. When CIS server analyzes a document, it looks for these terms, and determines whether to score a hit based on which terms it finds. For each document, CIS calculates the document score per category.

Each evidence term has a confidence value. The confidence value specifies how certain CIS server can be about scoring a hit for a document when it contains the term. The confidence values are also applicable when using category links as evidence for a category.

The following table illustrates the most common confidence values.

Table 98. Confidence values for evidence terms

<table>
<thead>
<tr>
<th>Confidence value (0 – 100)</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>High (75)</td>
<td>A term with high confidence is a strong evidence that a document belongs to the category. 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.</td>
</tr>
<tr>
<td>Medium (50)</td>
<td>A term with medium confidence is a good indicator that a document belongs to the category.</td>
</tr>
<tr>
<td>Low (15)</td>
<td>A term with low confidence only suggest that the category can 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.</td>
</tr>
</tbody>
</table>
### Confidence value (0 – 100)

<table>
<thead>
<tr>
<th>Confidence value</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Supporting</td>
<td>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.</td>
</tr>
<tr>
<td>Exclude</td>
<td>If one of the evidence terms found in a document has this confidence level, then the document is not assigned to the category. 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.</td>
</tr>
<tr>
<td>Required</td>
<td>These terms are must-have terms but they are not taken into account for the document score. If you define several required terms for a category, the document must contain at least one of them. 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.</td>
</tr>
</tbody>
</table>

If the document score exceeds or meets the category 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 to complete the assignment. If the score is lower than the candidate threshold, CIS server does not assign the document to the category.

**Related topics:**
- Providing evidence, page 387
- Defining evidence terms, page 399

### Category and taxonomy rules

The rules determine which documents are assigned to the categories. There are two types of rules:

- **Property rules**: Set conditions that a document must meet to be considered for assignment to the category. When set for categories, property rules can be used to assign documents. Property rules for a taxonomy cannot be used to assign documents but only to filter documents. For example, you can add a taxonomy rule to only analyze documents of a specific type. Any property rule associated with the taxonomy applies to every category within the taxonomy.

  Property rules are based on the repository attributes of the documents.

- **Evidence**: List the words, phrases, or patterns that CIS server looks for to indicate that a document belongs to the category. Evidence terms are identified in the content and/or in the metadata of the documents.

You can define only property rules, only evidence terms, or both. 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 contains both evidence terms and property rules, then both must be satisfied for a document to be assigned.

**Note:** Patterns are not defined in Documentum Administrator, the *EMC Documentum Content Intelligence Services Administration Guide* describes how to define patterns.

**Related topics:**
- Evidence terms, page 390
- Defining property rules, page 397
- Defining evidence terms, page 399

## Evidence terms

The evidence terms are the keywords and phrases that serve as evidence of the category.

The preferred evidence term is the category name. Other evidence terms can be synonyms of the category name to which you give the same confidence value or related terms to which you give a lower confidence value.

If you use only terms that are unique to that category, CIS server does not recognize the category in documents that relate to it in an indirect way. But if you choose common words as evidence terms, CIS server can recognize the category when the document does not belong to it.

The challenge is to create category definitions that are complete enough to trigger category recognition without introducing ambiguity. It is as important to keep misleading terms out of category definitions as it is to make sure that all viable terms are included.

Start with including proper nouns as evidence terms. When the proper noun is made up of several commonly occurring words, such as Internet Service Provider, define the term as a phrase. Collect the vocabulary from a set of documents representative of each category: synonyms, abbreviations, acronyms, antonyms, related terms that appear in the text.

**Note:** CIS server is not case sensitive for evidence terms.

**Related topics:**
- Providing evidence, page 387
- Category and taxonomy rules, page 389
- Defining evidence terms, page 399

## Using stemming on evidence terms

CIS server linguistic analysis module uses stemming to recognize grammatical forms of a word and treat them as a single evidence term. Stemming means extracting the common root, or stem, from words. For example, the words parked, parks, and parking share the same stem (park). The CIS server recognizes them as four instances of the same evidence term rather than as four different terms.
Turn off stemming when a common noun is used as a proper noun. 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. Also turn off stemming to treat different forms of the same stem as separate terms; for example, to use provider and provide as evidence of different categories.

When you turn off stemming, CIS server looks only for an exact match of the defined term. Explicitly add as terms all of the forms you want CIS server to recognize, such as plural forms or different forms of the verb.

You can activate the stemming at different levels:

- In the category class definition, you can use the stemming on the category names. If you select Use stemming in the category class definition, then it is the default value for all categories created from this category class.
- In the category definition, you can override the option inherited from the category class to use the stemming on the category names.
- For each evidence term, you can use the stemming, unless you selected Any language as the category language. In this case, the option is disabled.

Related topics:
- Evidence terms, page 390
- Defining evidence terms, page 399

Language detection for stemming

The language used for the stemming can be defined for the documents, for the categories, or for both of them.

The text of the document is analyzed and stemmed based on the language of the document set or, if not set, on the language_code attribute of the document, and if it is not set, on the detected 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. Defining a language for a category acts as a filter: a document is never assigned to a category of a different language. Similarly, if no language is set for a taxonomy or a category, all documents, regardless of the detected language, can match the category.

You can set the language at different levels:
- If all documents have the same language, set the language at the document set level.
- If the documents in a document set have different languages, let the CIS server detect the language.

On the category side, you can define the language at different levels:
- Set the language for the entire taxonomy.
- Set the language for every category.

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 evidence terms are stemmed in English.

If you do not set the language or if you set it as Any language for a category, documents in different languages can be assigned to this category. Use the Any language option if you do not 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. Setting the language of the category to Any language disables the stemming for the evidence terms of the category.

You can use the stemming for documents in English, French, German, Spanish, Italian, Brazilian Portuguese, Danish, Dutch, Norwegian, Swedish, Romanian, Russian, Finnish, Hungarian, or Turkish. When stemming is enabled, a language must be defined at the taxonomy or category level.

Related topics:
- Using stemming on evidence terms, page 390
- Document set language, page 406
- Defining taxonomies, page 394
- Defining categories, page 395

Reusing category evidence

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. This evidence propagation is done using category links. Like evidence terms, category links have a confidence value, telling CIS server how much to add to the document score for the current category when the document is assigned to the linked category.

For example, you can define a taxonomy with a first level of categories that is product-specific and subcategories for functional areas. To avoid defining evidence terms for the product in the subcategories, you can use the evidence defined for the parent category by setting a category link.

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 parent categories of this category into its set of evidence terms
- Child links, for which CIS links all children of this category into its set of evidence terms

To include automatically Parent or Child links, configure the category class. If a category belongs to a class where these options are set, the evidence for the category includes these links even though they do not appear in the category definition itself.

Related topics:
- Defining category classes, page 392
- Defining categories, page 395

Defining category classes

Each category refers to a category class. You can use the default category class called Generic or create one to set a specific configuration.
To create or modify a category class:

1. Navigate to Administration > Content Intelligence > Category Classes.

2. Select File > New > Category Class to create a category class, or click the icon next to the category class whose properties you want to set.

3. Enter a name and description for the category class.
   The name of the category class appears when you select a category class for a category. If you are editing a category class, the name is read only.

4. Select the document attribute into which CIS writes the names of assigned categories.
   The attribute must exist for the object type of documents that is categorized, and it must be a repeating value attribute, such as keywords. Each time a document is categorized, the attribute is updated. It means that CIS erases the current values and replace them with the result of the new categorization. Therefore, end users must not edit this attribute manually.

5. Click the Default Values tab.
   Use this page to set the default configuration for categories of this class. This configuration can be overridden in the category definition.

6. Specify how CIS treats the category name as an evidence term for the category.
   a. To use the category name as an evidence term, select Include Category Name as evidence term. If you deselect this option, go to step 7.
   b. To look for grammatical variations of the category name, select Use stemming.
   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.
   a. Select Use evidence from child/parent to apply evidence propagation to all categories for this category class.
   b. From the drop-down list, select child to use evidence from child categories as evidence for the current category or parent to use evidence from parent categories.

   Note: You cannot link to a category with a name that is not unique. If you define links to categories with a non-unique name, CIS ignore them during the processing.

8. Click Finish.

Related topics:
- Category classes, page 385
- Defining Content Intelligence Services configuration, page 381
- Using stemming on evidence terms, page 390
- Reusing category evidence, page 392
- Deleting category classes, page 404
Defining taxonomies

Create a taxonomy object before creating the categories in the hierarchy. The taxonomy object sets some default values for the categories below it.

Define one or several taxonomies. Define several taxonomies in the following cases:

• Define one taxonomy for each distinct subject area or domain.
• Maintain the taxonomies separately, by different subject matter experts, for example.
• Manage the taxonomies separately, for example, some taxonomies can be offline while others are online.

To create or modify a taxonomy:

1. Navigate to Administration > Content Intelligence > Taxonomies.
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 taxonomy.
   To modify a taxonomy, select it and select View > Properties > Info.
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.
5. Specify when the taxonomy settings as described in the following table:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>The taxonomy name is mandatory and must be unique. Once set, it cannot be modified.</td>
</tr>
<tr>
<td>Title</td>
<td>The title is not mandatory and it is not necessarily unique.</td>
</tr>
<tr>
<td>Description</td>
<td>The description is not mandatory.</td>
</tr>
</tbody>
</table>

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.
8. Select the taxonomy language.
The language of the taxonomy is used when the language of a category is not defined. If no language is set for the taxonomy, the evidence terms are stemmed in English. The selected language must match with the language of the documents that you want to classify.

9. Specify whether the taxonomy is online or offline.
   By default, a taxonomy is offline until you explicitly put it online by selecting Online from the State drop-down list.
   An online taxonomy is available for end users to browse and assign documents to. Keep the taxonomy offline until you have completed testing it.

10. Set the default on-target and candidate thresholds.
    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. Click the Property Rules tab to specify criteria that all documents in this taxonomy must meet.
    The procedure to define property rules for taxonomies is the same as defining property rules for categories. However, unlike property rules set for categories, the property rules for a taxonomy cannot be used to assign documents.
    The rules appear on the rules page for the category with the taxonomy name displayed in the title of the box.

12. Click OK to close the properties page.

13. Synchronize the new or modified taxonomy to make it available to CIS server.

Related topics:
- Taxonomies, page 384
- Defining category classes, page 392
- Defining property rules, page 397
- Synchronizing taxonomies with CIS server, page 400
- Displaying object titles, page 402

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 settings from the taxonomy or from the category class.

The following procedure describes how to create a category and set its basic properties.

To create a category:
1. Navigate to Administration > Content Intelligence > Taxonomies.
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 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 parent of the new category.

4. From the menu, select **File > New > Category**.

5. If you created subtypes, in the **Select Category Type** tab, select the category type from the drop-down list to create a subtype and click **Next**.

6. In the Attributes tab, specify when the category settings as described in the following table:

**Table 100. Taxonomy settings**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>The category name is mandatory and must be unique between categories that have the same parent. Once set, it cannot be modified. By default, the category name is the label that appears in the list of categories and the name of the folder created for this category. However, it is possible to display the category title instead of the category name. The maximum number of characters for the category name is 255 characters. The category path that includes the category name and the names of the parent categories must not exceed 450 characters.</td>
</tr>
<tr>
<td>Title</td>
<td>The title is not mandatory and it is not necessarily unique.</td>
</tr>
<tr>
<td>Description</td>
<td>The description is not mandatory.</td>
</tr>
</tbody>
</table>

7. Click the **Select owner** link and choose the owner of this category. The category owner is the user who can approve or reject documents assigned to the category as a candidate pending approval. The user you select is added to the ci_category_owner_role automatically, giving this user access to the category through Documentum Administrator.

8. Select the category class from the drop-down list.

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 are not assigned to the category. If you do not define the language of a category, and whatever the language of the parent category, the language set for the taxonomy is used. If no language is set for the taxonomy, the evidence terms are stemmed in English.

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. The default values come from the definition of the taxonomy you selected to navigate to this category.

11. Specify how CIS treats the category name as an evidence term for the category.
To use the category name as an evidence term, select Include Category Name as evidence term. If you deselect this option, go to step 12.

b. To look for grammatical variations of the category name, select Use stemming.

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. Specify how CIS uses evidence from child or parent categories.
   a. Select Use evidence from child/parent.
   b. From the drop-down list, select child to use evidence from subcategories of the current category or parent to use evidence from the parent category.

   Note: You cannot link to a category with a name that is not unique. If you define links to categories with a non-unique name, CIS ignore them during the processing.

13. If you created subtypes, click CustomProp tab to create a custom tab for the subtypes and enter the custom type for the subtype.

   If the customization for a subtype is not available, Documentum Administrator uses the closest supertype settings that are available for a particular subtype.

14. Click OK.

   The property page closes, and the category appears in the list.

15. To complete the category definition, set category rules.

Related topics:
- Categories, page 385
- Evidence terms, page 390
- Confidence values and score thresholds, page 388
- Reusing category evidence, page 392
- Defining property rules, page 397
- Displaying attributes in Property rules, page 402
- Displaying object titles, page 402

Defining property rules

Property rules define conditions that documents must meet to be assigned to the category.

To set property rules that documents must meet:
1. Navigate to Administration > Content Intelligence > Taxonomies.
2. Navigate to the taxonomy or category whose rules you want to set.

3. For a category, click the whistle icon  

   For a taxonomy, select View > Properties > Info.
4. From the Property Rules area, click the **Edit** link in the **Category Property Rule** box.

5. In the Property Rules page, to require assigned documents to come from a specific folder, click the **Select folder** link next to **Look in** and navigate to the folder.

6. 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 403, describes how to make custom object types available in the CIS component.

7. To assign documents based on their attributes, select the **Properties** checkbox and enter the criteria used to qualify documents.
   
   a. Select whether all criteria must 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 403, describes how to display custom attributes.

   c. Select the operator used to compare the selected attribute with the test value.
      
      The list of operators is updated based on the type of the selected attribute.
      
      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, enter the value as it appears in the Property page of the document. 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 a date attribute, the value must comply with Documentum date standards. **Table 101**, page 398 demonstrate a non-exhaustive list of possible date formats.

**Table 101. Date formats for property rules**

<table>
<thead>
<tr>
<th>Date format</th>
<th>Example</th>
</tr>
</thead>
<tbody>
<tr>
<td>mm/dd/yy</td>
<td>02/15/1990</td>
</tr>
<tr>
<td>mon DD yyyy</td>
<td>Feb 15 1990</td>
</tr>
<tr>
<td>mm/yy</td>
<td>02/90</td>
</tr>
<tr>
<td>dd/mm/yyyy</td>
<td>15/02/1990</td>
</tr>
<tr>
<td>yyyy/mm</td>
<td>1990/02</td>
</tr>
<tr>
<td>yy/mm/dd</td>
<td>90/02/15</td>
</tr>
<tr>
<td>yyyy-mm-dd</td>
<td>1990-02-15</td>
</tr>
</tbody>
</table>
Define evidence terms

Define words, phrases, and patterns as evidence terms for a category.

To define the properties of a category evidence term:

1. Navigate to Administration > Content Intelligence > Taxonomies.
2. Navigate to the category whose rules you want to set.
3. Click the whistle icon in the Rules column.
4. To add a term, click the Add a new simple term link.
   To modify a term, click the icon next to it.
5. To use a word or phrase as evidence for the category, click the Keyword button and type the word or phrase in the text box.
6. To use a pattern as evidence for the category, click the Keyword button and type the token value in the text box. The token value is defined in the patterns.properties file on CIS host, for example $Phone or $CreditCard.
7. To include another category as evidence for this category, click the Category Link button and identify the category to use as evidence for this category.
   • To use evidence from the hierarchical tree of the taxonomy, select Parent or Child from the drop-down list. Do not define a circular configuration between parent and children categories.
   • To link to a selected category, regardless of its position in the taxonomy, 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.

Note: You cannot link to category with a name that is not unique. If you define links to categories with a non-unique name, CIS ignore them during the processing.
8. For words or phrases, select **Use Stemming** to specify whether CIS server uses grammatical variations of the evidence term. This option is disabled if you selected Any language as the category language.

9. For a phrase, select **Recognize words in any order** to specify whether CIS server recognizes the phrase even if the words do not appear in the order you enter them.

10. Assign a confidence value for the evidence term.

    The confidence value indicates how certainly CIS server can infer the appropriateness of the category when the term appears in a document.

    The system assigns High confidence to the term by default. To specify a different value:
    
    a. Deselect the **Have the system automatically assign the confidence (HIGH) for me** option.
    
    b. To select a predefined confidence level, click **System Defined Confidence Level** and select a level from the list box.
    
    c. To set a custom confidence level, click **Custom Confidence Level** and enter a number from 0 through 100.

11. Click **OK**.

**Related topics:**

- Evidence terms, page 390
- Providing evidence, page 387
- Confidence values and score thresholds, page 388

## Synchronizing taxonomies with CIS server

When you create or modify any part of a taxonomy, synchronize it to make it available to CIS server.

**To synchronize a taxonomy definition:**

1. Navigate to Administration > Content Intelligence > Taxonomies.
2. Select the taxonomy you want to synchronize.
3. Select Tools > Content Intelligence > Synchronize.
4. Select if you want to synchronize the taxonomy with the production server, the test server, or both.
5. Click **OK** to start the synchronization.

    If you selected multiple taxonomies, click **Next** to select the 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. The *EMC Documentum Content Intelligence Services Administration Guide* provides the detailed 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 logged in CIS server log.
Related topics:
- Test processing and production processing, page 412
- Defining taxonomies, page 394
- Data synchronization between the repository and CIS server, page 382

Making taxonomies available

Bring a taxonomy online to make it available to end users. When a taxonomy is online, the taxonomy, its categories, and categorized documents appear to users under the Categories node in Documentum Administrator and in Webtop. The online/offline state is only applicable for taxonomies used for classic categorization.

To enable or disable a taxonomy to end users:
1. Navigate to Administration > Content Intelligence > Taxonomies.
2. Select the taxonomy and select View > Properties > Info.
3. Select the Attributes tab.
4. From the State drop-down list box, select Online to make the taxonomy available and display its categories. Select Offline to hide the categories.
5. Click OK.

Related topics:
- Test processing and production processing, page 412
- Defining taxonomies, page 394

Setting permissions for Content Intelligence

To define taxonomies, categories, category classes, or document sets in Documentum Administrator, you need Superuser privileges or the ci_taxonomy_manager_role. The following procedure describes how to restrict the access to the Content Intelligence node to only some members using the ci_taxonomy_manager_role.

To set permission using ci_taxonomy_manager_role:
1. Navigate to Administration > Administrator Access
2. Create an Administrator Access Set.
3. In the Administrator Access Set properties, select the Content Intelligence node and the role ci_taxonomy_manager_role.
5. Select the ci_taxonomy_manager_role.
6. Click File > Add Member(s) and select the names of the users or groups you want to add to this role.
7. Navigate to /System/Applications/CI and select all objects in the CI folder.
8. Open the object properties, and then the Permissions tab.
9. Select the Permission Set to CI Default ACL.

Related topics:
- Taxonomy manager, page 386
- Category owner, page 386

Displaying object titles

You can 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), you can display the title instead of the name. The titles are usually more user-friendly than names that are often used as an identifier.

You cannot choose to display only category titles, or only document titles. The switch applies to all objects. If the title is not defined for all objects then the column is 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.

Related topics:
- Defining taxonomies, page 394
- Defining categories, page 395
- Defining document sets, page 406

Displaying attributes in Property rules

To select which attributes to display for the property rules, modify the type list or the attribute list for 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, add them to an exclusion list. To make available attributes that are hidden by default, add them to an inclusion list.
Content Intelligence Services

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 <DA webapp directory>\webcomponent\config\admin\category.

2.

Open the qualifierrules_component.xml file.

3.

Under the <attribute_list> element, add an entry for the custom type whose attribute display
you want to modify or locate the <type id> element that exists for the dm_sysobject and
dm_document object types.
For example:
<attribute_list>
<type id='my_custom_type'>

4.

Under the <type id> element, add the attributes to display to the <inclusion_attributes> element,
and add the attributes to hide to the <exclusion_attributes> element.
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>

Related topics:
• Category and taxonomy rules, page 389
• Defining property rules, page 397

Creating subtypes for a taxonomy or a category
Create subtypes to add custom attributes to the taxonomies (dm_taxonomy objects) or to the
categories (dm_category objects). The subtype created resides in the repository data dictionary. They
inherit the ACL settings from dm_category and dm_taxonomy.
Use Documentum Composer to create the custom tab for the attributes of a category subtype. You
can configure the Documentum Administrator tab using Documentum Application Builder. After
configuring the Documentum Administrator tab, you can create a custom tab for their subtypes.

EMC Documentum Administrator Version 7.2 User Guide

403


If customization for a subtype is not available, Documentum Administrator uses the closest super-type settings that are available for a particular subtype.

Using Documentum Administrator and TEF, you can create a custom tab for the subtype.

Related topics:
- Defining taxonomies, page 394
- Defining categories, page 395

### Deleting category classes

When you delete a category class that is referenced by some categories, you must reassign the categories to another category class.

**To delete category classes:**

1. Navigate to Administration > Content Intelligence > Category Classes.
2. Select the category classes you want to delete.
3. From the File menu, select Delete.
4. For category classes that are referenced by categories, select another category class for the categories from the **Update categories to use the category class** drop-down list.
5. Click OK to delete the category class.

Related topics:
- Category classes, page 385
- Defining category classes, page 392

### 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.
2. Select the taxonomy to delete.
   
   A message page appears asking you to confirm that you want to delete the taxonomy.
4. Click OK.
Related topics:

- Taxonomies, page 384
- Defining taxonomies, page 394
- Reusing category evidence, page 392

Selecting and submitting the documents to analyze

This section contains the following topics:

- Document sets, page 405
- Document set language, page 406
- Defining document sets, page 406
- Configuring a document set, page 407
- Viewing the documents in a document set, page 408
- Scheduling a document set, page 408
- Synchronizing a document set, page 409
- Submitting documents to CIS server, page 410
- Submitting one document to CIS server, page 410
- Assigning a document manually, page 411

Document sets

Documents are submitted to the CIS server by batches called document sets. A document set is a collection of documents that are sent to the CIS server together, and which CIS server processes in the same way. Each document set has a definition to identify the documents applicable for this document set and a scheduling to determine when or how often the documents are processed.

The document sets can also have a configuration associated that defines the analysis performed (categorization, entity detection, and/or pattern detection). In this case, the analysis results are stored as annotations.

In an xCP environment, document sets are automatically created when associating discovered metadata to a content model. The document set is specific to a content model: analyzing a parent content model does not imply the analysis of inherited content models. The CIS server uses the document set to identify and process all instances of the model. If the content model is modified, the document set is updated during the redeployment. If all discovered metadata attributes are removed from the content model, the document set is deleted from the repository. All document sets defined for xCP are automatically scheduled to process content objects at regular intervals. This interval introduces a latency between a content object change and the update of its discovered metadata.
For classic categorization, create the document sets manually in Documentum Administrator. By default, the schedule of the document set is inactive. Define a schedule to run the document set automatically. Each time the document set runs, it submits only new or revised documents to CIS server.

**Related topics:**
- Document set language, page 406
- Defining document sets, page 406
- Configuring a document set, page 407
- Viewing the documents in a document set, page 408
- Scheduling a document set, page 408
- Synchronizing a document set, page 409
- Submitting documents to CIS server, page 410

### Document set language

The language selected for a document set must match the language of the categories and taxonomies used for categorization. The documents are never assigned to a category of a different language. If the language is not set for the category or taxonomy, any document of the document set can match, regardless of its language.

If the language of the document set is not defined, the CIS server detects it. If a document in the document set has a different language, it is ignored and the document is processed with the document set language.

**Related topics:**
- Document sets, page 405
- Language detection for stemming, page 391

### Defining document sets

Create a document set for classic categorization or when using the Annotations API to access analysis results.

In an xCP environment, document sets are automatically created when associating discovered metadata to a content model. The document set name is based on the content model name.

**To create a document set:**

1. Navigate to Administration > Content Intelligence > Document Sets.
3. In the Properties page, enter a name and description for the document set.
5. Schedule it as described in Scheduling a document set, page 408.

Related topics: Document sets, page 405

Configuring a document set

To configure a document set:
1. Navigate to Administration > Content Intelligence > Document Sets and select the document set.
2. Select View > Properties > Info.
3. In the Properties page, select the document set language.
4. Click the Document Set Builder tab. Specify the criteria for retrieving documents as described in the following table:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Look in:</td>
<td>To include documents from a specific folder, click Select next to Look in: and navigate to the folder containing the documents to process.</td>
</tr>
<tr>
<td>Type:</td>
<td>For classic categorization, to specify the object type of the documents selected for processing, click Select next to Type: and select the object type. In an xCP environment, the document set is automatically configured to process an object model.</td>
</tr>
<tr>
<td>Properties</td>
<td>Make sure Properties is already selected to assign documents based on their attributes. Enter the criteria used to select documents. For each rule, select an attribute, an operator and enter a value to test against. In an xCP environment, a rule is automatically added on the type to avoid processing objects whose type is inherited from the selected content model.</td>
</tr>
<tr>
<td>Add Property</td>
<td>To add another rule, click Add Property.</td>
</tr>
</tbody>
</table>
For classic categorization, you can test categorization by running the document set in test mode.

a. In the **Processing** tab, select **Test** as the Processing Mode.
   As a consequence, the CIS server set for the test mode is used.

b. Click **Select Taxonomy** and select a taxonomy to run the test against.
   For a test run, the CIS server only uses the taxonomy you are testing. The taxonomy does not need to be online. For a production run, all synchronized taxonomies are used for categorization.

c. When the test is done, switch the document set back to Production mode.

6. Synchronize the document set to make the changes available to the CIS server.

**Related topics:**

- Document sets, page 405
- Defining document sets, page 406
- Scheduling a document set, page 408
- Synchronizing a document set, page 409
- Displaying attributes in Property rules, page 402

### Viewing the documents in a document set

To view the documents included in the document set, navigate to **Administration > Content Intelligence > Document Sets** and double-click the name of the document set.

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 just from the document set.

**Related topics:**

- Document sets, page 405
- Submitting documents to CIS server, page 410

### Scheduling a document set

For classic categorization, schedule a document set to analyze new and modified documents regularly.

In an xCP environment, document sets are automatically scheduled to run every 15 minutes. They are set as active and are automatically synchronized. Modify the frequency of the scheduling and synchronize the document set.

**To schedule a document set:**

1. Navigate to **Administration > Content Intelligence > Document Sets**.
2. Select the document set you want to schedule.
4. Click the Processing tab.
5. Set the document set schedule to Active.
6. Specify when the documents should be submitted to the CIS server for processing as described in the following table:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Start Date</td>
<td>Set the day and time to indicate when the first run should happen.</td>
</tr>
<tr>
<td>Repeat</td>
<td>Set the frequency of the scheduling by typing a number in the Repeat box and selecting the time unit.</td>
</tr>
<tr>
<td>Processing Mode</td>
<td>For classic categorization, select the Processing Mode: Production or Test.</td>
</tr>
<tr>
<td></td>
<td>If you chose Test, click Select Taxonomy and select a taxonomy to run the test against.</td>
</tr>
</tbody>
</table>

7. Click OK.
8. Synchronize the document set to make it available to the CIS server.

Related topics:
- Document sets, page 405
- Defining document sets, page 406
- Configuring a document set, page 407
- Synchronizing a document set, page 409

Synchronizing a document set

After the creation and anytime you modify a document set, its configuration or its scheduling, synchronize it to make it available to the CIS server.

To synchronize a document set:
1. Navigate to Administration > Content Intelligence > Document Sets.
2. Select the document set you want to synchronize.
3. Select Tools > Content Intelligence > Synchronize.
   In the Synchronize page, CIS servers to Update shows which CIS server is updated based on the processing mode for this document set.
4. Click OK.
   If you receive any errors or warnings, refer to the error log on CIS server for details.
5. To check the status of the synchronization process, click **View Jobs** at the bottom of the page.
   When the synchronization is complete, a message indicating its success or failure is sent to your Documentum Inbox.

**Related topics:**
- Document sets, page 405
- Defining document sets, page 406
- Configuring a document set, page 407
- Scheduling a document set, page 408

### Submitting documents to CIS server

You can submit a document set to get it immediately processed by the CIS server.
For classic categorization, make sure the taxonomies are synchronized.

**To submit a document set for CIS server processing:**
1. Navigate to **Administration > Content Intelligence > Document Sets**.
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 disabled. 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**.
6. To review the status of a processing run, open the properties page for the document set and click the **Last Run** tab.
   Check the CIS server log files in the *EMC Documentum Content Intelligence Services Administration Guide* for a greater level of detail.

**Related topics:**
- Document sets, page 405
- Submitting one document to CIS server, page 410

### Submitting one document to CIS server

It is not possible to submit only one document in an xCP environment.
When you submit documents individually for classic categorization, the documents are added to a queue awaiting CIS server processing. They are processed as CIS server retrieves documents from the queue.
For classic categorization, make sure the taxonomies are synchronized.
To submit a document for CIS server processing:
1. Select the document that you want to categorize.
2. Select Tools > Submit for Classification.
Related topics: Submitting documents to CIS server, page 410

Assigning a document manually

You can manually assign a document from a cabinet folder to a category.

CIS server must be configured to Production mode. The Assign/Unassign option is not available in Test mode.

To assign a document manually:
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 selected attribute for the document.

Related topic:
- Test processing and production processing, page 412
- Switching from production view to test view, page 412
- Defining Content Intelligence Services configuration, page 381

Managing analysis results

This section contains the following topics:
- Test processing and production processing, page 412
- Switching from production view to test view, page 412
- Reviewing candidate documents, page 413
- Analysis results, page 414
- Category assignments, page 414
- Clearing category assignments for a taxonomy or category, page 415
• Clearing analysis results for a document set, page 415
• Clearing category assignments for a document, page 416

Test processing and production processing

With classic categorization, you can submit documents to CIS server in test mode or production mode. You choose the mode when you define the document set.

Although you can use the same CIS server for both production and testing, separate servers are recommended for better performance and availability. Offloading test processing from the production server prevents your tests from competing for resources with the production system.

You can view the documents assigned to a category either after a test processing or after a production processing.

In test mode, CIS server categorizes the documents, but it does not make any permanent update. Use the test mode to refine and validate your category definitions. The test mode allows you to specify the taxonomies you want to test. The taxonomy must be synchronized but does not need to be online. After reviewing the results of a test run, you can clear the proposed categorizations, update the category definitions, and run the test again.

In production mode, all synchronized taxonomies are used for categorization. The following actions can only be performed in production mode:

• Assigning a document manually.
• Reviewing documents pending approval.

CIS server updates documents and the repository based on the categorization results. Depending on the configuration, CIS performs the following updates:

• If the option Link to Folders is active, CIS server links documents into the folders corresponding to the categories.
• If the option Assign as Attribute is active, CIS server writes the name of the assigned categories into the specified document attribute.

Related topics:

• Defining Content Intelligence Services configuration, page 381
• Switching from production view to test view, page 412
• Clearing category assignments for a taxonomy or category, page 415
• Assigning a document manually, page 411
• Reviewing candidate documents, page 413

Switching from production view to test view

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.

Related topics:
- Test processing and production processing, page 412
- Assigning a document manually, page 411
- Reviewing candidate documents, page 413

Reviewing candidate documents

The category owner is responsible for approving or rejecting documents pending approval.

Documents receive Pending status when the confidence score that CIS server assigns to the document is higher than the category candidate threshold but lower than the 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 or CIS analyzes again the document after a change.

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.

2. Select My Categories with pending documents from the drop-down list in the upper right to display only categories that have pending documents.

3. To display the complete list of documents assigned to the category, click the Name of the category.

4. To display only Pending documents, click the value of the category in the Total Candidates column.

5. Select the checkbox next to the candidate document to select it.

6. To approve the document in this category, select Tools > Content Intelligence > Approve and click OK.
   If you are only viewing the Pending documents, the approved document disappears from the current view because it is no longer a candidate.

7. To reject the suggested categorization, select Tools > Content Intelligence > Reject Candidate and click OK.
   The document disappears from the current view because it is no longer a candidate.

8. Repeat steps 3 through 6 to review every document for all categories for which you are the category owner.

Related topics:
- Test processing and production processing, page 412
- Clearing category assignments for a taxonomy or category, page 415
Analysis results

Content Intelligence Services stores the analysis results in two ways:
- For classic categorization, analysis results are stored as category assignments.
- In an xCP deployment, analysis results are stored as annotations.

For classic categorization, you can manage category assignments in Documentum Administrator. You can clear assignments at the taxonomy level, at the category level, or for a single document. You can choose to clear only the documents in one category, or in the category and all of its children.

You can also clear analysis results (category assignments or annotations) for all documents belonging to a document set.

Clearing analysis results is most common when running during test phase. With classic categorization, where you can classify in production or in test mode, if you clear assignments made in production mode, any record of the category owner approval or rejection of a proposed assignment is also lost. As a result, CIS server asks again the category owner to approve or reject category assignments.

You can also access annotations using the Annotations API.

**Note:** When CIS categorizes an object, CIS updates its r_modify_date and r_modifier attributes. If the object does not satisfy categorization criteria, CIS does not modify the attribute values.

**Related topics:**
- Clearing category assignments for a taxonomy or category, page 415
- Clearing analysis results for a document set, page 415
- Clearing category assignments for a document, page 416

Category assignments

Category assignments are created as the result of the classic classification. A category assignment is a relationship between a document and the categories it is assigned to.

Content Intelligence Services can reflect category assignments in the repository 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. It allows users to see the documents in the taxonomy hierarchy.
- **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 for each matching category.

You can configure CIS to record category assignments in both ways, one of them, or neither. If neither Link to Folders or Assign as Attributes is active, Webtop users are not able to see the category assignments.

Category assignments and any of the related options are not available in xCP deployments.
Related topics:
• Analysis results, page 414
• Clearing category assignments for a taxonomy or category, page 415
• Clearing analysis results for a document set, page 415
• Clearing category assignments for a document, page 416

Clearing category assignments for a taxonomy or category

To clear category assignments of all documents in a taxonomy or category:
1. Navigate to Administration > Content Intelligence > Taxonomies.
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. Select one of the Clear assignments with status options to indicate to clear all assignments, only pending assignments, or only complete assignments.
   b. Select one of the Clear assignments with type options to indicate to clear test assignments, production 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.

Related topics:
• Analysis results, page 414
• Category assignments, page 414
• Clearing analysis results for a document set, page 415
• Clearing category assignments for a document, page 416

Clearing analysis results for a document set

This procedure is applicable to document sets for classic categorization and to document sets defined in xCP deployments.

To clear analysis results for all documents in a document set:
1. Navigate to Administration > Content Intelligence > Document Sets.
2. Navigate to the document set whose results you want to clear and select it.
3. Select Tools > Content Intelligence > Clear analysis results.
4. For classic categorization, select which types of assignments to clear.
a. Select one of the **Clear assignments with status** options to indicate to clear all assignments, only pending assignments, or only complete assignments.

b. Select one of the **Clear assignments with type** options to indicate to clear test assignments, production assignments, or both.

5. Click **OK**.
   If CIS is used to perform both classic categorization and categorization for an xCP deployment, all annotations are cleared as well as the selected category assignments.
   If CIS version is lower than 7.0, only category assignments are cleared.
   For classic categorization, a dialog box indicates how many categorization assignments are cleared.
   In xCP deployment, the dialog box indicates the name of the document set whose annotations are cleared.

6. Click **OK**.

**Related topics:**
- Analysis results, page 414
- Category assignments, page 414
- Clearing category assignments for a taxonomy or category, page 415
- Clearing category assignments for a document, page 416

### Clearing category assignments for a document

**To clear the assignment for a document:**

1. Navigate to Administration > Content Intelligence > Taxonomies.
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.

**Related topics:**
- Analysis results, page 414
- Category assignments, page 414
- Clearing category assignments for a taxonomy or category, page 415
- Clearing analysis results for a document set, page 415
Chapter 16

Resource Management

This chapter contains the following topics:

- Understanding Resource Management, page 417
- Managing resource agents, page 417
- Managing resource properties, page 420

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 first attempts to authenticate the user using the current session login information. If authentication fails, Documentum Administrator prompts for a user name and password.

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.

## Adding resource agents or modifying agent properties

Click the links below for information and instructions on:

- Adding resource agents, page 418
- Viewing or modifying resource agent properties, page 419

## 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.
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:
   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:
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:
   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.
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.
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 104. Start Operation page properties

<table>
<thead>
<tr>
<th>Field label</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Operation</td>
<td>Name of the operation</td>
</tr>
<tr>
<td>Description</td>
<td>Description of the operation.</td>
</tr>
<tr>
<td>Resource</td>
<td>Name of the resource.</td>
</tr>
<tr>
<td>Agent</td>
<td>Name of the resource agent.</td>
</tr>
<tr>
<td>Domain</td>
<td>Domain for the resource agent.</td>
</tr>
<tr>
<td>Parameters</td>
<td>The system will display input control fields if parameters are defined for the operation.</td>
</tr>
<tr>
<td>Start Operation</td>
<td>Click to invoke the operation. The dialog box remains open until you click Close.</td>
</tr>
<tr>
<td>Status</td>
<td>After the operation runs, displays that the operation completed or displays an error message, if one is provided.</td>
</tr>
<tr>
<td>Return Value</td>
<td>Displays the return value of the operation, if it has one.</td>
</tr>
<tr>
<td>Close</td>
<td>Close the dialog and return to the Resource Properties - Operations page.</td>
</tr>
</tbody>
</table>

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:
   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 105. Fields on the Notification page

<table>
<thead>
<tr>
<th>Field label</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Message</td>
<td>Notification message.</td>
</tr>
<tr>
<td>Occurred</td>
<td>Time notification occurred.</td>
</tr>
<tr>
<td>Resource</td>
<td>Name of the resource.</td>
</tr>
<tr>
<td>Agent</td>
<td>Name of the resource agent.</td>
</tr>
<tr>
<td>Domain</td>
<td>Domain for the resource agent.</td>
</tr>
<tr>
<td>Close</td>
<td>Close the dialog and return to the Resource Properties - Notifications page.</td>
</tr>
</tbody>
</table>

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:
   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.
   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.

   ```xml
   <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.

   ```xml
   <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>
   </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>
   </operations>
   <!--notifications are the list of notifications, ideally the empty list will capture all notifications.-->
   <notifications>
   ```
<notification></notification>
</notifications>
<!--refreshinterval denotes the interval in milliseconds for the monitor user interface to be refreshed. Ideal value should be 10sec.-->
<refreshinterval>10000</refreshinterval>
</mbeantype>
</mbeantypes>
Chapter 17

Administrator Access

This chapter includes the following topics:

- Administrator access sets, page 429

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.

In Documentum Administrator, the administrator access sets are managed on the Administrator Access Sets page. To access the Administrator Access Sets page, select Administration > Administrator Access.

Note: Administrator Access functionality is available only on Documentum 6 and later repositories.

Administrator access set definitions reside in the global registry. The access sets do not conflict with Content Server privileges. Object level and user level permissions and permission sets take precedence over administrator access sets. In general, administrator access sets control node access as follows:

- Users are not assigned an administrator access set and do not have superuser privileges, cannot access administration nodes.
- Users who are assigned an administration access set, but do no have superuser privileges, can only access the nodes that are enabled in their administration access set.
- Users with superuser privileges and at least coordinator client capabilities are not affected by administrator access sets. These users always have access to the entire administration node.
- The Groups node is always enabled for users with Create Group privileges.
- The Types node is always enabled for users with Create Type privileges.

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. If the same role name exists in both the global repository and a non-global repository, the user of the role would see the nodes as per the administrator access specified in the global repository. Even if the user is able to see the nodes, the user can perform operations only with sufficient privileges.
Note: The following Administration nodes are currently not available for the administrator access set functionality:

- Work Queue Management
- Distributed Content Configuration
- Privileged Clients
- Process Management
- My Documentum For Outlook

The User Management chapter provides information about setting up roles.

Creating, viewing, or modifying administrator access sets

Use the instructions in this section to create new administrator access sets. Only users with superuser privileges and Coordinator client capabilities or greater can create, view, or modify administrator access sets.

To create administrator access sets:

1. Connect to a repository with superuser privileges and client capability of Coordinator or greater.
3. Do one of the following
   - To create an administrator access set, select File > New > Administrator Access Set. The New Administrator Access Set - Info page displays.
   - To view or modify an administrator access set, select the access set, then select View > Properties > Info. The Administrator Access Set Properties page displays.
4. Enter or modify administrator access set information, as described in Table 106, page 430.
5. Click OK to save your changes.

Table 106. Administrator access set properties

<table>
<thead>
<tr>
<th>Field label</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>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.</td>
</tr>
<tr>
<td>Description</td>
<td>Description of the administrator access set.</td>
</tr>
<tr>
<td>Field label</td>
<td>Value</td>
</tr>
<tr>
<td>-------------</td>
<td>-------</td>
</tr>
</tbody>
</table>
| Nodes       | Select one or more node options to designate the nodes that users with this administrator access set can access. At least one node must be selected for an administrator access set. The available node options are:  
  - Basic Configuration  
  - LDAP Server Configuration  
  - Java Method Servers  
  - User Management  
  - Audit Management  
  - Jobs and Methods  
  - Content Objects  
  - Storage Management  
  - Content Delivery  
  - Index Management  
  - Content Intelligence  
  - Content Transformation Services  
  - Resource Management  

**Note:** To view the Content Intelligence Services node ensure that the repository is configured for it. If the repository is not configured, the Content Intelligence Services node will not appear. For detailed information on missing content intelligence node, refer **Missing Content Intelligence node**, page 382. |

**Assigned Role**

Indicates the role assigned to the administrator access set. If the role does not exist in the connected repository, the role is displayed in a red font.

To select or modify a role, click **Select** to select a role on the Choose a role page. The assigned role must be unique for an administrator access set or an error message displays, prompting the user to select a different role.

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. If an assigned role is missing in a connecting repository, the administrator access set does not apply for the missing role. Documentum Administrator displays a message notifying the user when an assigned role is missing.
Administrator access sets can be created without assigning a role, and they can contain an inactive or missing role. This is useful during the initial setup of your system.

## Deleting administrator access sets

Use the instructions in this section to delete administrator access sets. Only users with superuser privileges and Coordinator client capabilities or greater can 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.
Client Rights Management

This chapter contains the following topics:

- Client rights domains and privileged clients, page 433
- Client rights domains, page 433
- Privileged clients, page 437

Client rights domains and privileged clients

A client rights domain contains the Content Servers that share the same set of client rights objects. The client rights domain is configured in a global repository that acts as a governing repository. Multiple repositories can be grouped together under the global repository to share privileged DFC information. Privileged DFC is the term used to refer to DFC instances that can invoke escalated privileges or permissions for a particular operation. For example, privileged DFC can request to use a privileged role for an application to perform an operation that requires higher permissions or a privilege.

Client rights domains

A client rights domain is a group of repositories that share the same client rights. The group of repositories in a client rights domain is typically governed by a global repository (global registry). The following rules and restrictions apply to a client rights domain and repository members of that domain:

- A client rights domain can only be configured in a global repository.
- Only a global repository can be a governing repository.
- A global repository can only have one client rights domain.
- A global repository cannot be the governing repository and also a member repository of the client rights domain.
- A repository can only be a member of one client rights domain.
- The global repository must have access to all member repositories in the client rights domain.
- Changes to the client rights in the governing repository are automatically propagated to all member repositories in the same domain.
Creating a client rights domain

Creating a client rights domain requires superuser privileges and the repository on which you are creating a client rights domain must be a global registry.

**To add a client rights domain:**

1. In Documentum Administrator, navigate to Administration > Client Rights Management > Client Rights Domain to access the Client Rights Domain page.
3. Enter a name for the client rights domain in the Name field.
4. Select the Activate option to enable the client rights domain right now or do not select the option to enable the client rights domain at a later time.
5. Click OK to save your changes.

Enabling or disabling a client rights domain

Any modifications to a client rights domain require superuser privileges.

**To enable or disable a client rights domain:**

1. Navigate to Administration > Client Rights Management > Client Rights Domain to access the Client Rights Domain page.
2. Select the client rights domain, then select View > Properties > Info. The Client Rights Domain Properties page displays.
3. Do one of the following:
   - Select Activate to enable an inactive client rights domain.
   - Deselect Activate to disable an active client rights domain.
4. Click OK to save your changes.

Deleting a client rights domain

Deleting a client rights domain requires superuser privileges. Deleting a client rights domain also deletes associated member repository entries.

Deleting a client rights domain automatically starts dm_PropagateClientRights job, which removes the associated member repository entries. The job execution can take approximately 2 to 4 minutes and until the job has completed successfully, any member repository of the deleted client rights domain cannot be associated with another client rights domain.
To delete a clients rights domain:

1. Navigate to Administration > Client Rights Management > Client Rights Domain to access the Client Rights Domain page.
2. Select the client rights domain, then select File > Delete. You are prompted to confirm that you want to delete the clients rights domain.
3. Click OK to save your changes.

Adding member repositories

Adding a repository to a client rights domain requires superuser privileges.

To add a repository to a domain:

1. Navigate to Administration > Client Rights Management > Client Rights Domain to access the Client Rights Domain page.
2. Select the client rights domain, then select File > View > Member Repositories. The Member Repositories page displays.
4. Enter the information for the member repository as described in Table 107, page 435.
5. Click OK to save your changes.

Table 107. Member repository properties

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Member Repository Name</td>
<td>The name of the repository. The repository cannot be the governing repository (global registry).</td>
</tr>
<tr>
<td>Login Name</td>
<td>The login name of the repository user. The user must have system administrator privileges and be a member of the dm_sysadmin group.</td>
</tr>
<tr>
<td>Password</td>
<td>The password of the repository user.</td>
</tr>
<tr>
<td>User Login Domain</td>
<td>The name of the login domain for the user. Optional property.</td>
</tr>
<tr>
<td>Application Alias Name</td>
<td>The application name for the DFC instance. Optional property.</td>
</tr>
</tbody>
</table>

Viewing repository memberships

Viewing a member repository or modifying repository login information in a client rights domain requires superuser privileges.
To view a member repository:
1. Navigate to Administration > Client Rights Management > Client Rights Domain to access the Client Rights Domain page.
2. Select the client rights domain, then select File > View > Member Repositories.
   The Member Repositories page displays.
3. Select the member repository you want to view, then select File > View > Properties.
   The Properties page displays.
   You can view the member repository name and login name information. You can only modify the login name field value.
   If the domain name was specified when the repository was initially added to the client rights domain, the login name field also displays the domain name. In this case, you must enter the domain name with the login name using the same format:
   
   `<DOMAIN_NAME>\<LOGIN_NAME>`
   
   Make sure that you enter the correct domain name and login name. Content Server does not validate the domain or the login name. The new values are saved, even if they are invalid.
4. Click OK.

Removing a member repository from a client rights domain

Removing a member repository from a client rights domain requires superuser privileges. Removing a member repository also removes the client rights entries from the member repository.

Removing a member repository automatically starts dm_PropagateClientRights job, which removes the client rights entries from the member repository. The job execution can take approximately 2 to 4 minutes and until the job has completed successfully, the member repository cannot be associated with another client rights domain.

To remove a member repository:
1. Navigate to Administration > Client Rights Management > Client Rights Domain to access the Client Rights Domain page.
2. Select the client rights domain, then select File > View > Member Repositories.
   The Member Repositories page displays.
3. Select the member repository you want to remove, then select File > Delete.
   You are prompted to confirm that you want to remove the repository from the clients rights domain.
4. Click OK.
Privileged clients

Privileged DFC is the term used to refer to DFC instances that are recognized by Content Servers as privileged to invoke escalated privileges or permissions for a particular operation. In some circumstances, an application needs to perform an operation that requires higher permissions or a privilege than is accorded to the user running the application. In such circumstances, a privileged DFC can request to use a privileged role to perform the operation. The operation is encapsulated in a privileged module invoked by the DFC instance. Supporting privileged DFC is a set of privileged groups, privileged roles, and the ability to define TBOs and simple modules as privileged modules. The privileged groups are groups whose members are granted a particular permission or privileged automatically.

Each installed DFC has an identity, with a unique identifier extracted from the PKI credentials. The first time an installed DFC is initialized, it creates its PKI credentials and publishes its identity to the global registry known to the DFC. In response, a client registration object and a public key certificate object are created in the global registry. The client registration object records the identity of the DFC instance. The public key certificate object records the certificate used to verify that identity.

In Documentum Administrator, the privileged DFC clients are managed on the Privileged Clients page. To access the Privileged Clients page, select Administration > Client Rights Management > Privileged Clients.

The Privileged Clients page provides the following information:

Table 108. Privileged Clients page information

<table>
<thead>
<tr>
<th>Column</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Client Name</td>
<td>The name of the DFC client.</td>
</tr>
<tr>
<td>Client ID</td>
<td>A unique identifier for the DFC client.</td>
</tr>
<tr>
<td>Host Name</td>
<td>The name of the host on which the DFC client is installed.</td>
</tr>
<tr>
<td>Approved</td>
<td>Indicates if the given DFC client is approved to perform privilege escalations.</td>
</tr>
<tr>
<td>Manage Clients</td>
<td>The Manage Client button displays the Manage Client page, which lists all DFC clients that are registered in the global registry.</td>
</tr>
</tbody>
</table>

Adding privileged DFC clients, page 437 provides information about locating registered DFC clients and adding them as privileged DFC clients.

Configuring privileged client trusted login and trusted server privileges, page 438 provides information about trusted login and trusted server privileges.

Adding privileged DFC clients

The Manage Clients page displays the list of DFC clients created in the repository. When an you select one or more DFC clients as a privileged DFC client, a DFC client object is created in the logged in repository and displayed on the Privileged Clients page. The public key certificate is copied to the local repository.
Note: To add a privileged DFC client, you must be logged in as a superuser and you must be the owner of the dm_acl_superusers ACL or the install owner.

1. Navigate to Administration > Client Rights Management > 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.

   The Manage Clients page provides the following information:

   **Table 109. Manage Clients page information**

<table>
<thead>
<tr>
<th>Column</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Client Name</td>
<td>The name of the DFC client.</td>
</tr>
<tr>
<td>Client ID</td>
<td>A unique identifier for the DFC client.</td>
</tr>
<tr>
<td>Host Name</td>
<td>The name of the host on which the DFC client is installed.</td>
</tr>
<tr>
<td>Creation Date</td>
<td>The creation date of the DFC client.</td>
</tr>
</tbody>
</table>

3. To search for a DFC client, enter the name, or a portion of the name of the DFC client in the search field, then click .

   The system displays all registered DFC clients that match the criteria that you entered.

4. Select the registered DFC clients that you want to add as privileged clients, then click .

   The selected DFC clients move to the right side.

5. Click OK to return to the Privileged Clients list page.

### Configuring privileged client trusted login and trusted server privileges

Privileged Client trusted login and trusted server privileges are configured on the Privileged Client Properties page.

**To enable or disable trusted login and trusted server privileges:**

1. Navigate to Administration > Client Rights Management > Privileged Clients to access the Privileged Clients list page.

2. Click the Manage Clients button on the top right to access the Manage Clients page.

   Note: The Manage Clients button is disabled if a global registry is not configured or is unavailable.

3. Select the privileged client for which you want to enable or disable trusted login or trusted server privileges and select View > Properties > Info or right-click and select Properties.

   The Privileged Client Properties page displays.

4. Enable or disable trusted login or trusted server privileges, by selecting the Trusted Login and Trusted Server Privilege fields, as described in Table 110, page 439.
### Table 110. Privileged client properties

<table>
<thead>
<tr>
<th>Field label</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Client Name</td>
<td>The name of the DFC client.</td>
</tr>
<tr>
<td>Client ID</td>
<td>The unique identifier for the DFC client.</td>
</tr>
<tr>
<td>Host Name</td>
<td>The name of the host on which the DFC client is installed.</td>
</tr>
<tr>
<td>Client Privilege</td>
<td>Indicates whether the DFC client is approved to perform privilege escalations.</td>
</tr>
<tr>
<td>Trusted Login</td>
<td>Specifies whether the client is allowed to create sessions for users without user credentials.</td>
</tr>
<tr>
<td></td>
<td>Select this option to enable the client to create sessions for users without credentials.</td>
</tr>
<tr>
<td>Trusted Server Privilege</td>
<td>Specifies whether the DFC client is part of a trusted Content Server domain. If this option is enabled, the client has direct access to the repositories on the server.</td>
</tr>
<tr>
<td>Is globally managed</td>
<td>Select to propagate the privileged DFC information by domain. Optional property.</td>
</tr>
<tr>
<td>Application Name</td>
<td>The application name for the DFC instance. Optional property.</td>
</tr>
</tbody>
</table>

### Approving or denying privileged clients

DFC client privilege escalations are approved or denied on the Privileged Clients page.

**To approve or deny privileged clients:**

1. Navigate to Administration > Client Rights Management > 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 and add the DFC client, as described in Adding privileged DFC clients, page 437.
3. To approve a privileged DFC client, select the DFC client and do one of the following:
   - Select Tools > Approve Privilege.
   - Right-click and select Approve Privilege.
4. To deny a privileged DFC client, select the DFC client and do one of the following:
   - Select Tools > Deny Privilege.
   - Right-click and select Deny Privilege.
Deleting a DFC client and certificate

Use the instructions in this section to delete a DFC client and the certificate. You cannot delete a certificate that is also used by another DFC client.

To delete a DFC client and certificate:

1. Navigate to Administration > Client Rights Management > Privileged Clients to access the Privileged Clients list page.

2. Select the DFC client you want to delete and then right-click. From the available menu options, select Delete.

3. In the confirmation page, click OK to confirm or Cancel to exit.

Alternatively, you can also click Manage Clients in the Privileged Clients list page and then move the privileged DFC client back to the left column.
Chapter 19

Workflow Calendars

Processors 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. (The new calendar is effectively a copy of the base calendar. It does not inherit changes from the base calendar after creation.)

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.

The following sections provide instructions:
- Creating a calendar, page 441
- Editing a calendar, page 443
- Deleting a calendar, page 443

Note: To create/edit/delete workflow calendars using Documentum Administrator, the Process Engine has to be installed on the repository and user should have bpmuser role assigned. Otherwise, the Workflow Calendars node will not be visible under Administration.

Creating a calendar

Use the instructions in this section to create a calendar.

To create a new calendar:

1. In Documentum Administrator, navigate to Administration > Workflow Calendar. The Calendars page appears with a list of calendars that exist within the repository.
2. Click **Create Calendar**. A calendar-creation interface appears, with the **Calendar** tab forward.

3. To base the new calendar on an existing calendar, select the calendar name from the **Base calendar** list. The default is **None**.

4. Type a name for the calendar. You can also type a description.

5. Click **Next**. The **Periods** tab appears, allowing you to create separate periods of time.

6. Type a name for a period within the calendar.

7. Select a **Start date** and **End date** for this period.

8. Scroll down to display the **Working days** group of settings.

9. For at least one day of the week, select a **Start time** and an **End time**.

   **Note:** To set the same time for multiple working days, select the days of the week and then select **Use same time for all checked days**.

10. Scroll down to display the **Non-working days** group of settings.

11. If necessary, specify non-working days:
    - To identify a day as a non-working day, specify a date, optionally specify a name, and click **Add**. The date appears in the list of non-working days.
    - To edit a non-working day, select it from the list and click the **Edit** link. Change the date, change the name, or both. Click **Add** again. The list of non-working days is updated to reflect your changes.
    - To delete a non-working day, select it from the list and click the **Delete** link. The list of non-working days is updated to reflect your changes.

12. Click **Next**. The **Details** tab appears, displaying the list of events that are associated with the calendar.

13. If necessary, add, edit, or delete periods in your calendar:
    - To add a period to your calendar, click **Add**. The **Periods** tab reappears. Repeat the steps that apply to the **Periods** tab for each additional period in your calendar.
    - To edit a period in your calendar, select it and click **Edit**. The **Periods** tab reappears. Repeat the steps that apply to the **Periods** tab for each period that you want to edit.
    - To delete a period from your calendar, select it and click **Delete**. The period is removed from the list.

14. Click **Next**. The **Permissions** tab appears.

    Superusers can create, edit, or delete business calendars. Users with the bpmuser role can create business calendars and can edit or delete their own business calendars. Any user can see the business calendars created by others.

    Use this tab to manage the permissions for the business calendar.

15. Click **Finish**.

    The system saves the calendar to the /System/Workflow/Calendar folder.
Editing a calendar

Use the instructions in this section to edit a calendar.

**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 edit a calendar:**

1. In Documentum Administrator, navigate to Administration > Workflow Calendar. The Calendars page appears with a list of calendars that exist within the repository.
2. Right-click the calendar and select Properties. The calendar definition opens, enabling you to edit the calendar details.
   If the calendar is being used in a process, the system displays the process name on the Calendar tab, in the Process list.

Deleting a calendar

Use the instructions in this section to delete a calendar.

**Note:** The system will not delete a calendar that is referenced in any process definition.

**To delete a calendar:**

1. In Documentum Administrator, navigate to Administration > Workflow Calendar. The Calendars page appears with a list of calendars that exist within the repository.
2. Right-click the calendar and select Delete.
Chapter 20

Administering Business Processes

The Process Management node enables you to search for and then administer process templates and the associated process instances. This functionality makes it much easier to see how the system is doing at a glance and decide where to take corrective action, when necessary. Using Process Management, you can make changes to process instances without having to uninstall them first in Process Builder.

This chapter includes the following:

• Introduction to process management, page 446
• Finding process templates, page 446
• Administering process instances, page 449
• Administering tasks, page 451
Introduction to process management

The Process Management node gives you access to administrative functions for both process templates and process instances.

To display the process management node:
1. Start the Documentum Administrator user interface and log in.
2. Navigate to Administration > Process Management.

Note:
• To administer business processes using Documentum Administrator, the Process Engine has to be installed on the repository and user should have bpmuser role assigned. Otherwise, the Process Management node will not be visible under Administration.
• To view the process management related pages in Documentum Administrator, add the following in <DA>/WEB-INF/web.xml under the <web-app> tag:

```xml
<servlet>
  <servlet-name>InitServlet</servlet-name>
  <servlet-class>com.documentum.webcomponent.library.imaging.dashboard.servlets.InitServlet</servlet-class>
  <init-param>
    <param-name>DashboardProperties</param-name>
    <param-value>webcomponent/config/dashboard/dashboardProperties.xml</param-value>
  </init-param>
  <load-on-startup>5</load-on-startup>
</servlet>

<servlet>
  <description>Servlet for Dashboard SVG Process Diagram</description>
  <servlet-name>DashboardDiagramServlet</servlet-name>
  <servlet-class>com.documentum.webcomponent.library.imaging.dashboard.servlets.DashboardDiagramServlet</servlet-class>
</servlet>

<servlet-mapping>
  <servlet-name>DashboardDiagramServlet</servlet-name>
  <url-pattern>/dashboarddiagram/*</url-pattern>
</servlet-mapping>
```

Finding process templates

The Process Templates page shows a list of draft, validated, and installed process templates that exist within the repository.

In one or more search fields, type information about the process template that you want to find. You can also narrow the list of process templates by searching within the returned results for:
• Process name
• All processes, or those processes that are either installed or validated
• A specific version of the process
To search for a process template:

1. In Documentum Administrator, navigate to Administration > Process Management > Process Templates.
2. Type a search string in the Process Name field. Use the percent sign (%) as a wildcard.
3. To search for a process using a standard Version Label, do one of the following:
   - To select the current version, select the radio button and CURRENT from the list box.
   - To select all versions, select the radio button and ALL from the list box.
   - To select another version, select the radio button and type the version label in the text box.
4. Click Search to retrieve a list of processes that meet the search criteria.
5. To further filter the search results, select one of the following options from the list box:
   - Installed shows only installed processes.
   - Validated shows only validated processes.
   - All shows all processes saved in the repository, regardless of state.
6. Click Search to return a filtered list of results.
7. Select a process and click the Properties button to view the properties of the template.

This section also includes:
- Viewing process template properties search results, page 447
- Managing process templates, page 448
  - Managing process parameters, page 448
  - Starting a process, page 449
  - Viewing process instances, page 449

Viewing process template properties search results

The following table describes columns of returned information about the properties of the process templates:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>The name of the process as described in Process Builder.</td>
</tr>
<tr>
<td>Version</td>
<td>The Documentum version of the template.</td>
</tr>
<tr>
<td>Modified</td>
<td>Date that the template was last modified.</td>
</tr>
<tr>
<td>Instances</td>
<td>Number of workflows currently running and using this process template.</td>
</tr>
<tr>
<td>Longest Duration</td>
<td>The elapsed time of the longest running instance of this process.</td>
</tr>
<tr>
<td>Field</td>
<td>Description</td>
</tr>
<tr>
<td>------------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Audited</td>
<td>Indicates if auditing is turned on for the process.</td>
</tr>
<tr>
<td>Paused Tasks</td>
<td>Number of tasks that have been paused.</td>
</tr>
<tr>
<td>State</td>
<td>Indicates if the template is a draft or has been validated or installed.</td>
</tr>
<tr>
<td>Overdue Tasks</td>
<td>Number of tasks that are overdue.</td>
</tr>
</tbody>
</table>

**Managing process templates**

Once you have retrieved your list of process templates, you can manage the individual templates. The standard options such as access to the Process Properties are available from the right-click menu as well as the functions that are available as buttons on the page. For example, if there are process parameters associated with the process template, you can manage the parameters using either the right-click menu or the Manage Process Parameters button.

This section includes the following:

- Managing process parameters, page 448
- Starting a process, page 449
- Viewing process instances, page 449

**Managing process parameters**

Process parameters are constant values that you can modify while they are being used in a process. Process Parameter forms enable you to change a process parameter values from Documentum Administrator without having to change the original process in Process Builder.

Once you have retrieved the list of processes that meet the search criteria, you can view any process parameters that are associated with a process template. Process parameters can be used in thresholds, deadlines, escalation roles, and other values that are fixed across a process. When you change the values of the parameter, the value is updated for any new process instances or workitems. The process parameters in any currently running instances are not changed, although the values can change in any activity that occurs in the future.

If you have associated a custom form with the process parameters, the system displays the custom form with the list of process parameters that have been assigned to that template. If you have used a default form to display the parameters, the default form appears instead.

The *EMC Documentum Process Builder User Guide* provides details on creating process parameters. The *EMC Documentum Forms Builder User Guide* provides details on creating custom forms used to display process parameters.

**To view process parameters:**

1. Select a process name from the results list that has an associated Process Parameters form.
2. Click Manage Process Parameters to display the form that lists the process parameters.
The Manage Process Parameters button is only available for processes that have associated Process Parameter forms.

3. Edit the process parameter values by typing new values in the text box.

4. Click Submit to make the new parameters available to all new instances of the process.

Note: The system only updates process parameters that are changed in Process Builder or Documentum Administrator. Any changes you make to the process parameter default values in Forms Builder are ignored.

Starting a process

To start a process, select a process template and click Start. Attachments or packages (if specified) can be added to the process. Starting with the 7.0 release, there will be support for Business Objects (BO) which can be added as attachment or package. In the package selector, all the attributes of the BO will be visible making it easier for you to make a selection.

Viewing process instances

You can view all instances associated with the process by selecting a process template and clicking Show Instances. Using the default process instance search page, page 450 provides details on the functions available for administering process instances.

Administering process instances

A process instance is an entity that represents workflow or a process in runtime. Use the Process Instances node of the Process Management tree to search for specific instances of a process and to drill down and manage the details of that process instance.

The process instance list shows a list of process instances as well as other information about the state of each instance. This can be useful in determining if a process instance has aborted or is not running properly. From the list you can view all tasks in a given state, regardless of the process template that they are associated with. For example, you might want to find all paused tasks in the system and investigate the reason that they are paused.

The Process Instances node provides a default search page enabling you to find specific instances based up on the search fields.

This section includes the following:

- Using the default process instance search page, page 450
- Performing administrative functions for an instance, page 451
Using the default process instance search page

Documentum Administrator is delivered with a standard process instance search page that enables you to find processes based on a variety of search criteria.

To search for a process instance:

1. In Documentum Administrator, navigate to Administration > Process Management > Process Instances.
2. Enter search criteria in the search fields to retrieve a list of process instances.
3. Click Search.

The following table describes the fields you can use to search for a process instance.

**Table 112. Process Instance search fields**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Workflow name</td>
<td>The name of the process instance.</td>
</tr>
<tr>
<td>Supervisor name</td>
<td>A user with the role of supervisor for that particular instance.</td>
</tr>
<tr>
<td>Process name</td>
<td>The name of the process template.</td>
</tr>
<tr>
<td>Runtime State</td>
<td>Select one of the following workflow states:</td>
</tr>
<tr>
<td></td>
<td>• All</td>
</tr>
<tr>
<td></td>
<td>• Running</td>
</tr>
<tr>
<td></td>
<td>• Dormant</td>
</tr>
<tr>
<td></td>
<td>• Halted</td>
</tr>
<tr>
<td></td>
<td><strong>Note:</strong> In the custom search page, the value for Runtime State is typed in a text box. Valid values for the text box must be typed using the following format: SHOW_ALL, SHOW_DORMANT, SHOW_RUNNING, SHOW_HALTED</td>
</tr>
<tr>
<td>Version Label</td>
<td>The Documentum version of the process template.</td>
</tr>
<tr>
<td>Containing Tasks with</td>
<td>Select a value for the type of instances you want to appear in the search results.</td>
</tr>
<tr>
<td>Status</td>
<td>• All</td>
</tr>
<tr>
<td></td>
<td>• Failed</td>
</tr>
<tr>
<td></td>
<td>• Overdue</td>
</tr>
<tr>
<td></td>
<td>• Overdue and Failed</td>
</tr>
<tr>
<td></td>
<td>• Overdue or Failed</td>
</tr>
<tr>
<td></td>
<td><strong>Note:</strong> In the custom search page, the value for View Filter is typed in a text box. Valid values for the text box must be typed using the following format: SHOW_ALL, SHOW_FAILED, SHOW_OVERDUE, SHOW_OVERDUE_AND_FAILED, SHOW_OVERDUE_OR_FAILED.</td>
</tr>
</tbody>
</table>
If you have configured a custom search tab, the columns that appear in the search results are based upon the data you set up in the search page.

Performing administrative functions for an instance

The following buttons are enabled based upon the context of the instance and which actions are possible within a particular workflow.

Table 113. Buttons on Process Instances page

<table>
<thead>
<tr>
<th>Button</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Instance View</td>
<td>Enables you to drill down into the instance and see the process diagram as well as the list of tasks associated with the process instance. Administering tasks, page 451 provides more information on the process instance view.</td>
</tr>
<tr>
<td>Change Supervisor</td>
<td>Enables the administrator to select another supervisor from a list.</td>
</tr>
<tr>
<td>Resume Workflow</td>
<td>Starts this workflow and all its current tasks.</td>
</tr>
<tr>
<td>Halt Workflow</td>
<td>Pauses the workflow and pauses all of its current tasks.</td>
</tr>
<tr>
<td>Terminate Workflow</td>
<td>Stops the workflow without the option of restarting it.</td>
</tr>
</tbody>
</table>

Administering tasks

When you select a process instance and click the **Instance View** button from within the Process Instance search results page, the system displays the process diagram and associated tasks for the instance that you have selected. The instance view gives you a window into the running workflow and enables you to administer tasks for that workflow.

**Note:** If the browser does not display the instance view, you may need to download and install the Adobe Scalable Vector Graphics plugin. The plugin is available on the Adobe SVG Viewer download site.

You can click the individual activities within the process flow and the system highlights the associated task enabling you to see which tasks are associated with that activity. The instance view also shows icons that indicate the state of a particular activity within the instance. To see information about files that are attached to the workflow, select **Attachments**.

The *EMC Documentum TaskSpace User Guide* contains more information on tasks.

Table 114. Task properties

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Task Name</td>
<td>The name of the activity or the name of the sub-process associated with the instance.</td>
</tr>
<tr>
<td>Status</td>
<td>Displays the current status of the task.</td>
</tr>
</tbody>
</table>
The type of action that was performed on the task. For example, if the workitem was forwarded to another user, the action is *Forward*.

The name of the performer for the task. If the performer is based on a process parameter, the name is preceded and followed by a dollar sign ($), for example $Reviewer$.

Any comment or notations associated with the task.

The date the task was received by the task processor.

The date the task was completed by the processor.

When you right-click a task in the process instance view, you have the following options:

- Selecting **History** displays a list of events that have occurred to the item, such as checkout, checkin, and promote.

- Selecting **View** displays the Task Manager tabs which usually include the Info, Comments, and Progress tabs.

  The Info tab enables you administrator to take action on a process instance and task.

### Table 115. Administrative actions

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Previous</td>
<td>Displays the previous tab of the Task Info page.</td>
</tr>
<tr>
<td>Next</td>
<td>Displays the next tab of the Task Info page.</td>
</tr>
<tr>
<td>Get Task</td>
<td>Assigns the task to you and refreshes the page, enabling you to work on the task immediately.</td>
</tr>
<tr>
<td>Assign</td>
<td>Assigns the task to another user to complete.</td>
</tr>
<tr>
<td>Finish</td>
<td>Completes the task and sends it to the next step of the activity.</td>
</tr>
<tr>
<td>Delegate</td>
<td>Assigns another user the responsibility of performing a task that originally had been assigned to you.</td>
</tr>
<tr>
<td>Repeat</td>
<td>Sends the task to another user or group to repeat a task that you have just completed.</td>
</tr>
<tr>
<td>Perform</td>
<td>Executes the task.</td>
</tr>
<tr>
<td>Close</td>
<td>Closes the task.</td>
</tr>
<tr>
<td>Complete</td>
<td>Finishes the task and sends it to the next user or activity in the workflow.</td>
</tr>
<tr>
<td>Rerun</td>
<td>Runs automatic activities that have failed.</td>
</tr>
<tr>
<td>Reject</td>
<td>Sends the task to another step as defined in the template.</td>
</tr>
<tr>
<td>Suspend</td>
<td>Pauses the task in order to wait for some other supporting document or task to take place.</td>
</tr>
<tr>
<td>Unsuspend</td>
<td>Removes the task from the suspended state and enables the performer to acquire the task.</td>
</tr>
</tbody>
</table>
Depending on the type of activity, you can also perform management functions such as changing the performer, halting the workflow, editing timers, and so on.

### Table 116. Task properties

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Task Name</td>
<td>The name of the activity or the name of the sub-process associated with the instance.</td>
</tr>
<tr>
<td>Status</td>
<td>Displays the current status of the task.</td>
</tr>
<tr>
<td>Action</td>
<td>The type of action that was performed on the task. For example, if the workitem was forwarded to another user, the action is <em>Forward</em>.</td>
</tr>
<tr>
<td>Performer(s)</td>
<td>The name of the performer for the task. If the performer is based on a process parameter, the name is preceded and followed by a dollar sign ($), for example $Reviewer$.</td>
</tr>
<tr>
<td>Comment(s)</td>
<td>Any comment or notations associated with the task.</td>
</tr>
<tr>
<td>Receive Date</td>
<td>The date the task was received by the task processor.</td>
</tr>
<tr>
<td>Complete Date</td>
<td>The date the task was completed by the processor.</td>
</tr>
</tbody>
</table>

The **Process Variables** tab enables Administrator to provide values to the process variables added to a process, in xCP designer or Process Builder.

Process variables can be of either Simple Data Type or Structured Data Type (SDT) and they can be either single-valued or multi-valued (repeating). In Documentum Administrator, support has been provided to render multi-valued simple process variables under the **Process Variables** tab.

Values for multi-valued (repeating) process variables should be entered in new lines, which is used as a delimiter. For example, if you want to enter three values 10, 20, and 30 to a multi-valued process variable, it should be entered this way:

```
10
20
30
```

## Managing task details

The Task Details page gives you a high-level view of the task and shows the task identification number, any task instructions, the designated performer, and the priority number assigned to the task. If there are timers for the selected task, you can view them and update them, if necessary.

If timers exist for the selected task, they are grouped together based on their type. Timers that are created when the process instance is created are called **pre-task-creation timers**. **Pre-task-creation**...
Timers help to ensure that workitems are progressing to designated points in the workflow in a timely manner. A pre-task-creation timer takes action if an activity has not been triggered within a designated amount of time after the workflow starts. The activity is considered triggered once it is created by the workflow, but not necessarily acquired by a user. Pre-task-creation are not activated on the first activity of a workflow as they are automatically triggered during the workflow’s start.

Timers that are created after the task has been created are called post-task-creation timers. These timers help to ensure that a task is completed within a specified window of time after it has been started. A post-task-creation timer takes action if an activity has not completed within a designated amount of time after the activity starts.

Changes made to timers apply only to the selected task and not to other tasks based on the activity template. If the expiration of a timer is changed, any additional timers that follow in the task are not updated or changed in the same fashion. Their expiration times are completely independent. For example, if you add two hours to the first timer for a task, the system does not add two hours to the timers that follow.

When there are multiple timers for a task, the first timer is considered the due date for the task. (Documentum Administrator uses this due date to determine overdue tasks.) If you edit the expiration time for a subsequent timer to expire before the first timer, the due date of the task does not change. For example, if Timer_1 is set to expire at 10:00 AM and you edit Timer_2 to expire at 9:00 AM, the due date for the task remains 10:00 AM.

Note: Although the timer may be set to expire at a specific time, the action for that timer does not occur until the next time the timer job runs. The task of checking the warning timers and performing the requested actions is performed by the dm_WfmsTimer job. The EMC Documentum Process Builder User Guide provides more information on timers and the dm_WfmsTimer job.

To edit a task timer:

1. On the Instance Details page, click Task Details.
   The Task Details page shows the task timer name, any description or details for the timer, and the expiration time.

2. Select the timer with the values that you want to change and click Edit Timer.
   The Edit Timer page appears.

3. Use the calendar and time controls in the Expires field to set the new expiration values.
   To set the expiration to the current date and time, select the Set Timer Expiration as current time checkbox.

4. Click Show Job Info to view when the update timer job last ran and when the next job is scheduled to run.

5. Click Save to set the timer expiration to the new value.
Creating cabinets

Cabinets display the highest level of organization in a repository. Cabinets contain folders, and files.

To create a cabinet:
1. Navigate to the repository in which to create the cabinet.
2. Select the Cabinets node, then select File > New > Cabinet
4. In the Create tab, type the name of the cabinet, and type of cabinet.
5. In the **Info** tab, specify properties if required. All properties in the Info tab are optional.

6. In the **Permissions** tab, specify the access that users, and groups have to the cabinet, as described in **Table 117, page 456**.

7. Click **Finish**.

**Table 117. Permissions tab for cabinets, folders, and files**

<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Your Permissions</td>
<td>The permissions you have for this cabinet, folder, or file. The Permissions of owner or superuser is a function of the permissions of dm_owner, dm_world, group permissions, restrictions on user/group, and so on and is not solely dependent on the value of associated dm_acl object.</td>
</tr>
<tr>
<td>Permission Set Name</td>
<td>The name of the default permission set that is assigned to this cabinet, folder, or file. To change the permission set, click <strong>Select</strong> and select a different permission set from the permission set list.</td>
</tr>
<tr>
<td>Permissions Set Owner</td>
<td>The name of user that owns the permission set that is assigned to the cabinet, folder, or file.</td>
</tr>
<tr>
<td>Description</td>
<td>A description of the permission set. The default description is the object ID of the permission set.</td>
</tr>
<tr>
<td>Additional Permissions</td>
<td>Specifies other users and groups that have permissions for this cabinet, folder, or file. By default, all users (dm_world) have a Read permission and only the cabinet, folder, or file owner (dm_owner) has a Delete permission.</td>
</tr>
</tbody>
</table>

To add or change permissions:
- To add users or groups, click **Add** and assign the desired permissions.
- To change the permissions for a user or group, select the user or group and click **Edit**.
- To remove a user or group, select the user or group and click **Remove**.
### Property Description

<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Restrictions</td>
<td>Specifies the access restrictions for specific users and groups. Click <strong>Restriction</strong> to expand and view the restricted users and groups.</td>
</tr>
<tr>
<td></td>
<td>To add or change restrictions:</td>
</tr>
<tr>
<td></td>
<td>• To add users or groups, click <strong>Add</strong> and assign the desired restrictions.</td>
</tr>
<tr>
<td></td>
<td>• To change the restrictions for a user or group, select the user or group and click <strong>Edit</strong>.</td>
</tr>
<tr>
<td></td>
<td>• To remove a user or group, select the user or group and click <strong>Remove</strong>.</td>
</tr>
<tr>
<td>Advanced Permissions</td>
<td>Specifies groups and group set memberships that are required to access the cabinet, folder, or file. If IRM is installed on the repository, you can also specify IRM permissions.</td>
</tr>
<tr>
<td></td>
<td>Click <strong>Advanced Permission</strong> to expand and view the required user and group memberships. To add a required group, click <strong>Add</strong> and select the group and group set.</td>
</tr>
<tr>
<td>Search</td>
<td>Displays permissions for users and groups. Click <strong>Search</strong> and select a user or group, then click <strong>OK</strong>. The system displays the permissions that are currently assigned to that user or group.</td>
</tr>
</tbody>
</table>

### Creating folders

**To create a 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.
4. In the **Info** tab, specify properties if required. All properties in the Info tab are optional.
5. In the **Permissions** tab, specify the access that users, and groups have to the folder, as described in Table 117, page 456.
6. Click **Finish**.

### Creating files

**To create a file:**

1. Navigate to the folder in which to create the new file.
2. Select **File > New > Document**.
3. In the **Info** tab, enter the file properties as described in Table 118, page 458.
4. In the **Info** tab, specify file properties if required. All properties in the Info tab are optional.
5. In the **Permissions** tab, specify the access that users, and groups have to the folder, as described in **Table 117**, page 456.
6. Click **Finish**.

**Table 118. Info tab for documents**

<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Specifies the name of the document.</td>
</tr>
<tr>
<td>Type</td>
<td>Specifies the file type. Select a file type from the drop-down list.</td>
</tr>
<tr>
<td></td>
<td>If the file type you want to create is not available, you can create a file of that type on your local machine and import the file into the repository.</td>
</tr>
<tr>
<td>Format</td>
<td>Specifies the file format. Select a format from the drop-down list.</td>
</tr>
<tr>
<td></td>
<td>If the file format you want to create is not available, you can create a file of that format on your local machine and import the file into the repository.</td>
</tr>
<tr>
<td>Template</td>
<td>Specifies a file template. Select a template from the drop-down list.</td>
</tr>
<tr>
<td></td>
<td>If the template you want to use to create the file is not available, you can use a template on your local machine to create the file and import the file into the repository.</td>
</tr>
<tr>
<td>Show Options</td>
<td>Click to expand the Options menu. Check the <strong>Subscribe to this file</strong> option to receive email notifications if the file is modified.</td>
</tr>
</tbody>
</table>

**Creating a form**

When you create a form, the form is based on a template. Form templates are generally created using Documentum Forms Builder and stored in the repository. You cannot use Documentum Administrator to create a template. To use form functionality, you must have the form_user rule assigned.

**To create a form:**
1. Navigate to where you want to create the form.
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. Enter the form data.
Working with files

Checking out files

When you check out a file, Documentum Administrator either copies or streams the file to your computer, depending on the editing application that is used for the file. 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, Documentum Administrator uses the following checkout directory:

- On Windows machines: //Documentum/Checkout
- On Macintosh machines: Root:Users:user_name:Documentum:Checkout

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 the following:
   - 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.

Checking in files

When a file is checked in and versioned, the file renditions, including any thumbnail renditions, are not maintained with the new version of the file. The renditions remain with the previous version. Any parent document of the versioned file 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. Enter the appropriate checkin information, as described in Table 119, page 460. Checkin information varies depending on the repository configuration.

5. Click OK or Next, depending on whether you are checking in one or multiple files. To apply information to all remaining files at once, click Finish.
### Table 119. Checkin information

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Save as</td>
<td>Sets the version number. Selecting the same version number overwrites the original file with the updated one.</td>
</tr>
<tr>
<td>Version label</td>
<td>Lets you label the updated version.</td>
</tr>
<tr>
<td>Description</td>
<td>Lets you write an optional description of the file.</td>
</tr>
<tr>
<td>Format</td>
<td>Defines the type of file.</td>
</tr>
<tr>
<td>Lifecycle ID</td>
<td>Assigns a lifecycle to the file.</td>
</tr>
<tr>
<td>Check for links to other Microsoft documents, and check in linked documents</td>
<td>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.</td>
</tr>
<tr>
<td>Upload options</td>
<td>Determines how quickly the new content is available to other users, and whether you can use Documentum Administrator during the checkin operation.</td>
</tr>
<tr>
<td></td>
<td><strong>Note:</strong> If you used drag-and-drop you are not given this option.</td>
</tr>
<tr>
<td></td>
<td>Select one of these:</td>
</tr>
<tr>
<td></td>
<td>• <strong>Send for immediate global access:</strong> Updates the repository immediately for all your organization's users. While this occurs, you cannot perform other actions in Documentum Administrator.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Send first for local access:</strong> 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.</td>
</tr>
<tr>
<td></td>
<td><strong>Note:</strong> 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.</td>
</tr>
<tr>
<td>Show Options Retain Lock</td>
<td>Saves the updated file to the repository but keeps the file checked out in your name.</td>
</tr>
<tr>
<td>Make this the current version</td>
<td>Makes the updated file the current version.</td>
</tr>
<tr>
<td>Field</td>
<td>Description</td>
</tr>
<tr>
<td>-----------------------------</td>
<td>----------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Keep a local copy after</td>
<td>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.</td>
</tr>
<tr>
<td>checkin</td>
<td></td>
</tr>
<tr>
<td>Subscribe to this file</td>
<td>The file is linked to your Subscriptions.</td>
</tr>
<tr>
<td>Check in from file</td>
<td>Replaces the repository file with a file you choose.</td>
</tr>
</tbody>
</table>

**Viewing 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.

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 uses multiple repositories, My Files also displays the files you have recently accessed from other repositories. You can perform all the standard operations on files from other repositories, so long as you have usernames, and passwords for those repositories.

**Canceling checkout**

Canceling a 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. Click **OK** or **Next**, depending on whether you cancel the checkout for one or for multiple files. To confirm cancellation for all remaining files at once, click **Finish**.

**Versioning**

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. 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.

- 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.

**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.

If you edit an earlier version of a file, you have the following options when you checkin the file:

- You can check in 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 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.

**Moving files**

You can move files to another location within the same repository. By default, Documentum Administrator moves only the selected version.

You cannot move an file that is locked. If a file is locked, the lock owner must first unlock it.

**Tip:** You can also move files 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 files.
2. Select **Edit > Add To Clipboard**.
   **Tip:** You can add files from multiple locations to your clipboard. All files on your clipboard are moved to the same location.
3. Navigate to the location to which to move, and open the location to display the content pane. Select **Edit > Move Here**.
Copying files

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 files.
2. Select Edit > Add To Clipboard.
   Tip: You can add files from multiple locations to your clipboard. All files on your clipboard are copied to the same location.
3. If you are copying files to another repository, open that repository in the navigation pane.
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. Select the files to copy and click Copy.
   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.

Viewing files 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 a directory on your local machine. By default, the copy is stored in the C:\Documentum\Viewed 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. 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.

Importing folders and files

If you import a folder, the content of the folder is also imported.

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**.

3. Specify file properties, if applicable, as described in **Table 120, page 464**. The table describes common properties. Your installation of Documentum Administrator might include different properties.

4. Click **OK** or **Next**, depending on whether you are importing one file or multiple files. To apply the selected properties to all remaining files at once, click **Finish**.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Type</td>
<td><em>Do not change this property</em></td>
</tr>
<tr>
<td>Format</td>
<td><em>Do not change this property</em></td>
</tr>
<tr>
<td>Lifecycle ID</td>
<td>Assigns a lifecycle to each imported item.</td>
</tr>
<tr>
<td>Check for links to other Microsoft documents,</td>
<td>If this field appears, check this to have Documentum Administrator scan each import 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.</td>
</tr>
<tr>
<td>and import linked documents</td>
<td></td>
</tr>
<tr>
<td>Upload options</td>
<td>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:</td>
</tr>
</tbody>
</table>

- **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.

- **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.

### Exporting folders and files

You can export a folder or individual files.
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 entire content of the folder is exported, including subfolders.

**To export a folder or file:**

1. Navigate to the files or folders you want to export.
2. Select the files or folder, then 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 and click **OK**.
4. Specify export options, if applicable.
5. If the file or folder already exists on the local machine, do one of the following:
   - Click **Yes** to overwrite or **No** to cancel overwriting a specific file or folder on the local machine.
   - Click **Yes to all** to overwrite or **No to all** to cancel overwriting all existing files or folders.

**Linking cabinets, folders, or files**

Links can be used to associate items in the repository with different locations or repositories. You can also email links.

You can link cabinets, folders, or files to:

- A location in the repository
  - When you link an item to a 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.
- Another repository
  - You can link an item from one repository to another. The link 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. To navigate from the shortcut to the original item, select the shortcut, and then select **File > Go to Target**
- A location on the local machine

**To link an item to a location:**

1. Select one or more items.
2. Select **Edit > Add To Clipboard**.
   - **Tip:** You can add items from multiple locations to your clipboard. All items on your clipboard are linked to the same location.
3. Open the location to which to link to display the content pane, then select **Edit > Link Here**.
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.

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.

To link a repository item to your computer:

1. 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 a folder on your computer.

Viewing all linked locations for an item

To view all locations to which an item is linked:

1. Select the item.
2. Select View > Locations or select View > Memberships.

Bookmarking a document or folder

To add a document or folder to your browser’s bookmarks or favorites:

1. Select the document or folder.
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.
Sending a link in an email message

To send a link in an email message:
1. Select one or more items in the repository.
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.

Viewing the clipboard

Your clipboard holds the files you are moving, copying, or linking to another location in the repository.
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.

Deleting cabinets, folders, or files

To delete a cabinet, folder, or file:
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. Click OK or Next, depending on whether you are deleting one or multiple items. To apply the selected properties to all remaining items at once, click Finish.

Managing 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 to a repository item:
1. Select the item.
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. Select the item.
2. Select Tools > Subscribe Others.
3. In the selection dialog box, select one or more users, and click OK.

**To cancel your subscription to an item:**
1. Select the item.
2. Select Tools > Unsubscribe.

### Enabling change notifications

**To enable change notifications:**
1. Select one or more files.
2. Do one of these:
   - To receive a notification whenever a file is opened, checked out, or exported, select Tools > Turn on read notification.
   - To receive a notification whenever a file is changed, select Tools > Turn on change notification.

   Notifications are sent to both your Documentum Administrator inbox, and your email inbox.

To turn off notifications, select the file, and select either Tools > Turn off read notification or Tools > Turn off change notification.

### Managing relationships

A relationship is a connection between two objects in a repository. Relationships allow Documentum Administrator to process the objects together. Relationships also allow users to access certain objects by first accessing other related files. 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 relationships:**
1. Select the object.
2. Select View > Relationships.

**To create a relationship between two items:**
1. Select the object that becomes the parent.
2. Right-click the file, and select Add Relationship.
3. In the selection area, select the object to relate to this object, and click OK.
4. Click Next.
5. In the Relationship list, select the type of relationship.
6. Click Finish.
To remove a relationship between two files:
1. Select either of the objects.
2. Select View > Relationships.
3. Select the relationship to remove.
4. Click File > Remove Relationship.
5. Click OK.

Renditions and transformations

A rendition is a copy of a file in a different format. For example, a rendition can be a copy of an image in a different file format or in a different resolution. Renditions can be generated using Documentum Administrator or imported into the repository.

Note: Some rendition and transformation functionality is available only on repositories that are configured with EMC Documentum's Content Transformation Services products.

Viewing file 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. Select View > Renditions.

Importing a rendition

You can 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 file format for the rendition 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 a user views the object. However, any rendition can be used as the default rendition. For example, for a large, high resolution image file, a smaller, low-resolution image can be used as the default rendition.

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. 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.

Transforming a document to PDF or HTML format

Documentum Administrator requires EMC Documentum Content Transformation Services products to provide the functionality to transform documents to PDF or HTML format. When processing is complete, a new file in either PDF or HTML format is stored in the object’s list of renditions.

The status of transformation requests is displayed in the Transformations node of the navigation tree. An indicator also appears next to files that have transformation requests:
- A yellow indicator (_yellow) indicates that the file has a pending transformation request.
- A green indicator (_green) indicates that a transformation request is currently processing.
- A red indicator (_red) indicates that a transformation request has failed.

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.

Enabling inbox notification

User can receive notifications in their Inbox when the transformation is complete by enabling this feature in their preferences.
To enable inbox notification of transformations:
2. Navigate to the General tab.
3. Select the check box for Turn Inbox Notification options on.

Configuring PDF Annotation Service

If EMC Documentum PDF Annotation Service is installed with Content Server, users can store comments created in Adobe Acrobat or Reader into a repository, as well as 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.

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.

Virtual documents

In a Documentum repository, a virtual document is a file that contains one or more nested files. The virtual document is also called the parent document, and the nested files are called descendants or children. The nested files can themselves be virtual documents, providing multiple levels of nesting.

A virtual document can contain descendants of different file formats. For example, a Microsoft Word parent file can contain an Excel spreadsheet, and TIFF image as descendants.

Creating a virtual document

To create a virtual document, you use Documentum Administrator to 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. In Documentum Administrator, select the file to be converted.

Virtual documents may also be created programmatically. The basic steps to create a virtual document programmatically are:

1. Obtain the object that you want to use as a virtual document.
   Folders and cabinets cannot be virtual documents.
2. Set the object's r_is_virtual_doc property.
   Setting this property is optional. If users are never going to open or work with the document, setting this property is not necessary. However, setting it ensures that if users do work with the document, the document behaves appropriately.
3. Add components to the object.
   Two methods add components to a virtual document: IDfSysObject.appendPart andIDfSysObject.insertPart. The appendPart method adds components to the end of the ordered list of components that make up the virtual document. The insertPart method inserts components into the ordered list of components at any location. Note that neither method sets the r_is_virtual_doc property. They only increment the r_link_cnt property.
4. Save or check in the object.
   The permissions required to write the object to the repository vary depending on how it was obtained:
   - If you created a new object, use a save method to put the object in the repository.
   - If you used a fetch method to obtain the object, use a save method to save the changes to the repository.
     You must have Write permission on the virtual document to save the changes you made.
   - If you used one of the checkout methods to obtain the object, use one of the checkin methods to save your changes to the repository.
     You must have at least Version permission on the virtual document to use checkin. If the repository is running under folder security, you must also have Write permission on the object's primary cabinet or folder.

Refer to the associated Javadocs for information about the methods used to add or remove components or update a virtual document component.

Viewing the structure of a virtual document

When you view the structure of a virtual document in Documentum Administrator, Virtual Document Manager (VDM) opens to display the 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.

**Viewing virtual document content**

When you view the content of a virtual document in Documentum Administrator, the content opens in an editing application.

If the repository includes XML functionality, you can view both the parent, and descendants in a single, read-only XML file. If there is no content in a virtual document, then Virtual Document Manager (VDM) automatically displays the virtual document structure.

**To view the content of a virtual document in read-only mode:**
1. Select the virtual document in Documentum Administrator.
2. Select File > Open (Read Only).

**Assembling a virtual document**

Typically, users work on individual parts of a virtual document, retrieving them from the repository as needed. However, eventually, they need to work with the parts as one document. The process of selecting individual components to produce a virtual document is called assembling a virtual document.

1. Use a SELECT statement to retrieve the object IDs of the components from the repository.
2. Use the object IDs to get the components from the repository.
   - After obtaining the components, the application can manipulate the components as needed.

In the context of an application, assembling a virtual document has two steps:

Which component objects are selected depends on the following:
- how the objects are bound to the virtual document
- the criteria specified in the SELECT statement (including the IN DOCUMENT clause late binding condition, if any)
- for those components that are themselves virtual documents, how their assembly behavior is defined

Using the SELECT statement SEARCH and WHERE clauses and the WITH option in the IN DOCUMENT clause, you can assemble documents based on current business rules, needs, or conditions.

For example, perhaps your company has an instruction manual that contains both general information pertinent to all operating systems and information specific to particular operating systems. You can put both the general information and the operating system-specific information in one virtual document and use conditional assembly to assemble manuals that are operating system-specific.
The following SELECT statements use a WHERE clause to assemble two operating system-specific manuals, one Linux-specific, and the other VMS-specific:

```
SELECT "r_object_id" FROM "dm_document"
IN DOCUMENT ID('0900001204800001') DESCEND
WHERE ANY "keywords" = 'Linux'
```

```
SELECT "r_object_id" FROM "dm_document"
IN DOCUMENT ID('0900001204800001') DESCEND
WHERE ANY "keywords" = 'VMS'
```

Notice that the virtual document identified in both IN DOCUMENT clauses is the same. Each SELECT searches the same virtual document. However, the conditions imposed by the WHERE clause restrict the returned components to only those that have the keyword Linux or the keyword VMS defined for them.

The use_node_ver_label and follow_assembly properties affect any components that are themselves virtual documents. Both control how Content Server chooses the descendants of such components for inclusion.

### Processing the SELECT statement

This section describes the algorithm Content Server uses to process a SELECT statement to assemble a virtual document. The information helps you to write a SELECT statement that chooses exactly the components you want.

Content Server uses the following algorithm to process a SELECT statement:

1. The server applies the criteria specified in the SEARCH and WHERE clauses to the document specified in the IN DOCUMENT clause. The order of application depends on how you write the query. By default, the SEARCH clause is applied first. When a document meets the criteria in the first clause applied to it, the server tests the document against the criteria in the second clause. If the document does not meet the criteria in both clauses, the SELECT returns no results.

2. The server applies the criteria specified in the SEARCH and WHERE clauses to each direct component of the virtual document. The order of application depends on how you write the query. By default, the SEARCH clause is applied first. When a component meets the criteria in the first clause applied to it, the server tests it against the criteria in the second clause. If a component does not meet the criteria in both clauses, it is not a candidate for inclusion.

   If a component is late bound, the SEARCH and WHERE clauses are applied to each version of the component. Those versions that meet the criteria in both clauses are candidates for inclusion.

3. The binding condition in the WITH option is applied to any versions of late-bound components that passed Step 2.

   It is possible for more than one version to meet the condition specified by the WITH option. In these cases, the server uses the NODESORT BY option to select a particular version. If NODESORT BY option is not specified, the server includes the version having the lowest object ID by default.

4. If the DESCEND keyword is specified, the server examines the descendants of each included component that is a virtual document. It applies the criteria specified in the SEARCH and WHERE clauses first.
For late-bound descendants, the SEARCH and WHERE clauses are applied to each version of the component. Those versions that meet the criteria are candidates for inclusion.

5. For late-bound descendants, the server selects the version to include from the subset that passed Step 4. The decision is based on the values of use_node_ver_label in the containment objects and the binding condition specified in the WITH option of the IN DOCUMENT clause.

The resulting set of components comprises the assembled document.

The WITH option and the SEARCH and WHERE clauses are optional. For example, if you do not specify the WITH option and the search encounters any late-bound components, the server takes the version having the lowest object ID or, if NODESORT BY is specified, whichever is first in the sorted order.

If you include an IN ASSEMBLY clause instead of an IN DOCUMENT clause, the server applies the SEARCH and WHERE clauses to the components found in the specified snapshot. Similarly, if you include the USING ASSEMBLIES option in the IN DOCUMENT clause or if the component has follow_assembly set to TRUE, when the server finds a component that has a snapshot, it applies the SEARCH and WHERE clauses to the objects in the component snapshot rather than recursively searching the component hierarchy.

### Setting a version label for a virtual document

**To set a version label for a virtual document:**

1. In Documentum Administrator, navigate to the virtual document and select it.
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.

### Creating a virtual document archive

An archived version of a virtual document is called a snapshot.

**To view a list of snapshots created for a virtual document:**

1. In Documentum Administrator, navigate to the virtual document and select it.
2. Select View > Snapshots.

**To create a snapshot:**

1. In Documentum Administrator, navigate to the virtual document and select it.
3. Enter information in tabs as appropriate.
4. Click **Finish**.

Typically, snapshots are created through Virtual Document Manager. However, it is possible to create them programmatically. The basic steps are:

1. Content Server uses an IDfSysObject.assemble method to select the components for the snapshot and places them in a collection.

   **Note:** If you include the interruptFreq argument in the assemble method, you cannot execute the method inside an explicit transaction. (An explicit transaction is a transaction explicitly opened by an application or user.)

2. Content Server executes an IDfSession.getLastCollection method to obtain the ID of the collection holding the components.

3. Content Server executes an IDfCollection.next method to generate assembly objects for the components.

4. When the next method returns a NULL value, Content Server executes an IDfCollection.close method to close the collection.

   The collection must be explicitly closed to complete the snapshot creation. If you close the collection before all the components have been processed (that is, before assembly objects have been created for all of them), the snapshot is not created.

**To freeze or unfreeze a snapshot:**

1. Select the snapshot in Documentum Administrator.

2. Do one of the following:
   - **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.

**Converting 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. In Documentum Administrator, navigate to the virtual document.

2. Remove all descendants from the virtual document, if applicable.

3. Select the virtual document.

**Setting virtual document preferences**

To set your virtual document preferences:

1. In Documentum Administrator, select Tools > Preferences.

2. Select the Virtual Documents tab, and complete the fields in Table 121, page 477.

**Table 121. Virtual document preferences**

<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Opening options</td>
<td>Specifies how a virtual document is opened. This option does not apply if the virtual document is already opened in Virtual Document Manager (VDM):</td>
</tr>
<tr>
<td></td>
<td>• <strong>View structure</strong>: The first level of nested files appears.</td>
</tr>
<tr>
<td></td>
<td>• <strong>View content</strong>: A read-only copy of the content appears.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Prompt each time</strong>: The user is prompted to select to display the structure or the read-only content.</td>
</tr>
<tr>
<td></td>
<td>If there is no content in a virtual document, the VDM automatically displays the virtual document structure, regardless of the preference.</td>
</tr>
<tr>
<td>Bindings</td>
<td>Specifies whether VDM shows broken bindings. A binding is broken if VDM cannot find the version of a component specified by the associated binding rule.</td>
</tr>
<tr>
<td>Copy</td>
<td>Specifies how a virtual document is copied to the clipboard:</td>
</tr>
<tr>
<td></td>
<td>• <strong>Root only</strong>: Copies the content, and properties of the parent file only.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Root and descendants</strong>: Copies the parent file, and all the descendants nested in the parent file, including descendants of descendants.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Root and link to existing descendants</strong>: Copies the parent file, and references the descendants.</td>
</tr>
</tbody>
</table>
### Property Description

- **Prompt me each time**: Prompts the user to select what to copy.
- **Checkout**: Specifies how a locked document is checked out:
  - **Download as read-only**: Downloads a copy of the item as read-only.
  - **Prompt me each time**: Prompts the user to select whether to download as read-only.

3. Click **OK** to save the preferences.

## Obtaining information about virtual documents

This section describes how to query a virtual document and how to obtain a path through a virtual document to a particular component.

### Querying virtual documents

To query a virtual document, use DQL just as you would to obtain information about any other object. Documentum provides an extension to the SELECT statement that lets you query virtual documents to get information about their components. This extension is the IN DOCUMENT clause. Used in conjunction with the keyword DESCEND, this clause lets you:

- Identify all components contained directly or indirectly in a virtual document
- Assemble a virtual document

Use the IN DOCUMENT clause with the ID scalar function to identify a particular virtual document in your query. The keyword DESCEND directs the server to search the virtual document full hierarchy.

**Note**: The server can search only the descendants of components that reside in the local repository. If any components are reference links, the server cannot search the descendents of the referenced documents.

For example, suppose you want to find every direct component of a virtual document. The following SELECT statement does this:

```sql
SELECT "r_object_id","object_name" FROM "dm_sysobject"
IN DOCUMENT ID('virtual_doc_id')
```

This second example returns every component including both those that the document contains directly and those that it contains indirectly.

```sql
SELECT "r_object_id" FROM "dm_sysobject"
IN DOCUMENT ID('virtual_doc_id') DESCEND
```
The VERSION clause lets you find the components of a specific version of a virtual document. The server searches the version tree that contains the object specified in virtual_doc_id and uses (if found) the version specified in the VERSION clause. For example:

```
SELECT "r_object_id" FROM "dm_sysobject"
IN DOCUMENT ID('virtual_doc_id') VERSION '1.3'
```

### Obtaining a path to a particular component

If you are writing web-based applications, the ability to determine a path to a document within a virtual document is very useful. One property (path_name) and methods in the IDfSysObject interface provide this information.

### The path_name property

The path_name property is defined for the assembly object type. When you create a snapshot for a virtual document, the processing automatically sets each assembly object path_name property to a list of the nodes traversed to arrive at the component represented by the assembly object. The list starts with the top containing virtual document and works down to the component. Each node is represented in the path by its object name, and the nodes are separated with forward slashes.

For example, suppose that Mydoc is a virtual document and that it has two directly contained components, BrotherDoc and SisterDoc. Suppose also that BrotherDoc has two components, Nephew1Doc and Nephew2Doc.

If a snapshot is created for Mydoc that includes all the components, each component will have an assembly object. The path_name property values for these assembly objects would be:

- Mydoc, for the Mydoc component
- Mydoc/BrotherDoc, for the BrotherDoc component
- Mydoc/BrotherDoc/Nephew1Doc, for the Nephew1Doc component
- Mydoc/BrotherDoc/Nephew2Doc, for the Nephew2Doc component
- Mydoc/SisterDoc, for the SisterDoc component

The path_name property is set during the execution of the next method during assembly processing. If the path is too long for the property length, the path is truncated from the end of the path.

Because a component can belong to multiple virtual documents, there may be multiple assembly objects that reference a component. Use the assembly object book_id property to identify the virtual document in which the path in path_name is found.

### Using DFC

In DFC, use the IDfSysObject.vdmPath and IDfSysObject.vdmPathDQL methods to return the paths to a document as a collection. Both methods have arguments that tell the method you want only the paths found in a particular virtual document or only the shortest path to the document.
The vdmPathDQL method provides the greatest flexibility in defining the selection criteria of late-bound versions found in the paths. The vdmPathDQL method also searches all components in the paths for which the user has at least Browse permission.

With vdmPath, you can only identify version labels as the selection criteria for late-bound components in the paths. Additionally, vdmPath searches only the components to which World has at least Browse permission.

**Email messages**

New email messages are imported as dm_document type or its subtypes and in Outlook Message Format (.msg) to the repository. Also, other email management functions have changed. The *EMC Documentum Webtop 6.8 User Guide* contains the detailed information.
This chapter includes the following topics:

- Inboxes, page 481
- Opening a task or notification, page 482
- Performing a task, page 482
- Completing a task, page 482
- Accepting a group task, page 483
- Rejecting a task, page 483
- Delegating a task, page 484
- Repeating a task, page 484
- Changing availability for tasks, page 484
- Work queue tasks, page 485

Inboxes

The Documentum Administrator Inbox contains tasks, and notifications. All repository users have their own individual inbox. Tasks are electronic assignments and can include attached files. Notifications are messages that an event has occurred.

A task can be assigned 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 a user completes a workflow task, the workflow automatically sends a task to the next user in the workflow. If an organization uses work queues, users can request task assignments.

Note: For accessing all process or workflow related tasks in the inbox, install Process Engine on the repository.
Opening a task or notification

To open a task or notification:
1. Click Inbox.
2. Click the name of the task or notification.
3. Perform the task or click Close to close the task or notification.

Performing a task

To perform a task:
1. In your Inbox, click the task to open it.
2. On the Info tab:
   • Perform operations on attached files as required.
   • To attach additional files, click Add Attachments, select the files, and click OK.
   • If the Time, and Cost fields appear, record your time, and cost to perform the task.
   • 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.
3. In the Comments tab, add comments as follows:
   a. Click Add or Edit and type a comment in the Comment field.
   b. Send the comment, using one of the following options:
      • 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.
   c. Click OK.
4. Select the Progress tab to view task’s history.
5. Do one of the following:
   • Mark the task as finished.
   • 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.

Completing 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.
   c. Click OK.
6. If prompted, select the next task to forward from the Select Next Forward Tasks list.
7. Click OK.

Accepting a group task

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 inbox of the other users.

To accept a task that has been assigned to multiple users:
1. Click Inbox.
2. Select the task to accept.
3. Click Accept.
4. Perform the task.

Rejecting 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. Whether the task remains in the Inboxes of the other users in the group depends on the template definition.

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.

Delegating 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**.
4. Click **OK**.

Repeating 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**.
5. Click **OK**.

Changing 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 **I am available** or **I am currently set to unavailable**.
3. Do one of the following:
   • 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.

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 users 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. Users 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 their Inbox.
Chapter 23

Search

This chapter includes the following topics:

- Searches, page 487
- Setting search preferences, page 487
- Search guidelines, page 488
- Running a simple search, page 489
- Running an advanced search, page 492
- Viewing search results, page 495
- Additional configuration options, page 498
- Saved searches, page 499
- Creating a search template, page 500

Searches

Documentum Administrator offers different ways to search repositories and external sources. By default, Documentum Administrator provides a simple search and an advanced search. If Federated Search Services is installed on the Content Server host, administrators also have the option to create search templates and configure smart navigation.

The *EMC Documentum Federated Search Services Installation Guide* provides more information about installing Federated Search Services.

Setting search preferences

Search preferences specify the default search locations and enable smart navigation.

To set your search preferences:

1. Select **Tools > Preferences**.
2. Select the **Search** tab.
3. In the **Default Search Locations** area, do one of the following:
   - 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 Federated Search Services are installed on Content Server.

5. To save your changes, click **OK**.
   - To select the columns displayed in the result pages, set your column preferences.
   - To retrieve the default configuration of the search locations, and of smart navigation, click **Restore defaults**.

### Search guidelines

In general, the following guidelines apply to searches:

- If a document cannot be indexed, it also cannot be searched. For example, documents that contain binary content cannot be indexed.
- Only certain characters can be searched, such as alphabetic, numeric, extender, and custom characters. Custom characters include Chinese, Japanese, Korean letters, and months.
  - Other characters, including punctuation, accent, and diacritical marks, and characters such as `!` and `#`, are not indexed or searched. These characters are removed from the indexed text and are treated as blank spaces. The xPlore federation treats characters such as `!@#$%^&;:()+=<` as white space.
- The plus and minus signs cannot be used as operators. You must use the AND operator, and the OR instead.
- The asterisk, and the question mark can be used as wildcards.
Running a simple search

When a user enters 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.

A full-text search searches the files in default search location that the user is specified in the search preferences. The search can include several repositories at the same time and external sources such as external databases, web sources or the desktop.

When displaying search results, Documentum Administrator displays files with the most matching words first. If a repository has been indexed for parts of speech, Documentum Administrator also displays files that include variations of the words. For example, if a user searches for scanning, 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.
   Further define search terms, page 489 provides the detailed information to further define your search.
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. Viewing search results, page 495 provides the detailed information.

Further define search terms

You can use the syntax in Table 122, page 489 to further define search terms within a simple search or within the Contains field in an advanced search.

Table 122. Further define search terms

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Quotation marks around a word or phrase: “ “</td>
<td>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 scanning for the word scanner. 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.</td>
</tr>
<tr>
<td>Syntax</td>
<td>Description</td>
</tr>
<tr>
<td>------------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>The <strong>AND</strong> and <strong>OR</strong> operators</td>
<td>To get results that contain two search terms, type <strong>AND</strong> between the terms. A term can be a word or quoted phrase.</td>
</tr>
<tr>
<td></td>
<td>To get results that contain at least one term, type <strong>OR</strong> between the words or the quoted phrases.</td>
</tr>
<tr>
<td></td>
<td>You can string together multiple terms with the <strong>AND</strong> and <strong>OR</strong> operators. The <strong>AND</strong> operator has precedence over the <strong>OR</strong> operator. For example, if you type:</td>
</tr>
<tr>
<td></td>
<td><strong>AND</strong> between the terms. A term can be a word or quoted phrase.</td>
</tr>
<tr>
<td>The <strong>NOT</strong> operator</td>
<td>To get results that do not contain a term, type <strong>NOT</strong> before this term. The term can be a word or quoted phrase. Only the term that follows the operator is taken into account.</td>
</tr>
<tr>
<td></td>
<td>The <strong>NOT</strong> operator can be used after the <strong>AND</strong> or <strong>OR</strong> operator, separated by a space.</td>
</tr>
<tr>
<td></td>
<td>Valid syntaxes would be: Documentum <strong>NOT</strong> adapter or Documentum <strong>AND</strong> <strong>NOT</strong> adapter, both queries will return results that contain Documentum but do not contain adapter.</td>
</tr>
<tr>
<td></td>
<td>If you type Documentum <strong>OR</strong> <strong>NOT</strong> adapter, you get results that either contain Documentum (and possibly contain adapter) or that do not contain adapter. Use this syntax cautiously. It can generate a very large number of results.</td>
</tr>
<tr>
<td></td>
<td>The <strong>NOT</strong> operator can be used alone at the beginning of the query. For example, if you type <strong>NOT</strong> adapter, you get results that do not contain adapter. Use this syntax cautiously. It can generate a very large number of results.</td>
</tr>
<tr>
<td></td>
<td>The <strong>NOT</strong> operator is not supported for queries on external sources when it is alone at the beginning of the query or if used with the <strong>OR</strong> operator.</td>
</tr>
<tr>
<td></td>
<td>The <strong>NOT</strong> operator cannot be used with parentheses. This is invalid: <strong>A NOT ( B OR C ).</strong> However, the <strong>NOT</strong> operator can be used inside parentheses. This is valid: (<strong>A NOT B</strong>) <strong>OR</strong> (<strong>A NOT C</strong>).</td>
</tr>
<tr>
<td></td>
<td><strong>ANDNOT</strong> (in one word) is not an operator, if you enter <strong>ANDNOT</strong> in a query, it will be considered as a search term.</td>
</tr>
<tr>
<td>Syntax</td>
<td>Description</td>
</tr>
<tr>
<td>--------</td>
<td>-------------</td>
</tr>
</tbody>
</table>
| Parentheses around terms: () | To specify that certain terms must be processed together, use parentheses. When using parenthesis, you must type a space before, and after each parenthesis mark, as shown here: (management or discovery)  
As an example, if you type knowledge and management or discovery, then your results will contain both knowledge, and management or they will contain discovery. But if you type knowledge and (management or discovery), then your results will contain knowledge, and either management or discovery. |
| The multiple-character wildcard: * | 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).  
The multiple-character wildcard is not available for a searches on non-indexed repositories, for searches of property values, or for searches of external sources. For those, you should use truncation operators, such the Begin with operator.  
**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  
d*ment  
then your results must contain: document, development, deployment, department, etc. but not documented or documentation. |
| The single-character wildcard: ? | If the repository is indexed, you can use the single-character wildcard to indicate a single, unknown character anywhere in a word.  
The single-character wildcard is only available or a simple search (including the Contains field in an advanced search).  
The single-character wildcard is not available for searches on non-indexed repositories, for searches of property values, or for searches of external sources. |

**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.
Running 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. Entering values for an advanced search, page 492 provides the detailed information.
3. Click Search.
   
   Tip: To stop the search, in the result page, click Stop.

Entering values for an advanced search

This procedure assumes you have already opened the Advanced Search page. If you have not, see Running an advanced search, page 492.

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.
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 123, page 493 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 123. Common properties in an advanced search

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Properties list</td>
<td>Enter one or more property values to search for by doing these:</td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>1. If no fields appear, click Select a property.</td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>2. On a given line: In the first drop-down list, select a property. In the</td>
</tr>
<tr>
<td></td>
<td>second drop-down list, select a property-to-value relationship. Table 124,</td>
</tr>
<tr>
<td></td>
<td>page 494 provides the description of possible relationships. In the</td>
</tr>
<tr>
<td></td>
<td>remaining fields, select or type values. If you type multiple words, they</td>
</tr>
<tr>
<td></td>
<td>are searched for as a phrase. For example, if you type &quot;knowledge</td>
</tr>
<tr>
<td></td>
<td>management&quot; then Documentum Administrator searches for values that contain</td>
</tr>
<tr>
<td></td>
<td>the phrase &quot;knowledge management&quot; but not for values that contain</td>
</tr>
<tr>
<td></td>
<td>&quot;knowledge&quot; and &quot;management&quot; separated from each other by other words such</td>
</tr>
<tr>
<td></td>
<td>as &quot;knowledge and process management&quot;. If you want your results to</td>
</tr>
<tr>
<td></td>
<td>include both terms either as a phrase or separately, you must create</td>
</tr>
<tr>
<td></td>
<td>two subqueries, and use the AND operator.</td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>3. To add additional properties, click Add another property, and</td>
</tr>
<tr>
<td></td>
<td>then select one of these operators:</td>
</tr>
<tr>
<td></td>
<td>• And: Selecting this means that the search results must match both</td>
</tr>
<tr>
<td></td>
<td>the property value on this line, and the property value on the previous</td>
</tr>
<tr>
<td></td>
<td>line.</td>
</tr>
<tr>
<td></td>
<td>• Or: Selecting this means that the results can match either the</td>
</tr>
<tr>
<td></td>
<td>property value on this line or the property value on the previous line.</td>
</tr>
<tr>
<td></td>
<td>If you search external sources, do not use the OR operator between</td>
</tr>
<tr>
<td></td>
<td>different types of properties. This query is valid: &quot;Author contains</td>
</tr>
<tr>
<td></td>
<td>Lewis OR Author contains Twain,&quot; but this query is not valid: &quot;Author</td>
</tr>
<tr>
<td></td>
<td>contains Lewis OR Name contains Knowledge management.&quot;</td>
</tr>
</tbody>
</table>

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 "Name contains Knowledge Management AND Author contains Lewis OR Author contains Twain," 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:
Search

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td><em>Author contains Lewis OR Author contains Twain AND Name contains Knowledge management.</em></td>
</tr>
</tbody>
</table>

4. To remove a property from the search criteria, click **Remove** for that property.

**Date**

Select the type of date to search for. Specify a date range, either a fixed date range using today’s date or by typing the **From** and/or **To** dates. Months can be written in figures or in full. Years can be written with two or four figures.

When specifying a date **From**, the date is not included in the date range. Conversely, when specifying a date **To**, the date is included in the date range.

**Size**

Select a size range.

*Properties when searching for email messages*

- **Subject**: Type the words for which to search.
- **To**
- **From**
- **Sent**: Select the date the email message was sent.
- **Received**: Select the date the email message was received.

**Find hidden objects**

Choose to include hidden items in the search. The search displays only those hidden items that you have permission to view.

**Find all versions**

Choose to search for past versions of the file, as well as the current version.

The relationship between a property, and its corresponding value is defined by operators. **Table 124, page 494** describes the operators available in the Advanced Search page.

**Table 124. Select a property-to-value relationship**

<table>
<thead>
<tr>
<th>Operator</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Relational operators:</strong></td>
<td>You can use these operators with numerical values or strings.</td>
</tr>
<tr>
<td>Less than &lt;</td>
<td></td>
</tr>
<tr>
<td>Less than or equal to &lt;=</td>
<td></td>
</tr>
<tr>
<td>Greater than &gt;</td>
<td></td>
</tr>
<tr>
<td>Greater than or equal to &gt;=</td>
<td></td>
</tr>
<tr>
<td>Equal to =</td>
<td>Returns results in which the property value contains only the exact value you typed.</td>
</tr>
<tr>
<td>Not equal &lt;&gt;</td>
<td>Returns results in which the property value never matches the value you typed.</td>
</tr>
</tbody>
</table>

**Truncation operators:**

The truncation operators can be used in place of the multiple-character wildcard.
<table>
<thead>
<tr>
<th>Operator</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Begins with</td>
<td>Returns results in which the property value begins with the value you typed. Same as using an ending wildcard.</td>
</tr>
<tr>
<td>Ends with</td>
<td>Returns results in which the property value ends with the value you typed. Same as using an starting wildcard.</td>
</tr>
<tr>
<td>Contains</td>
<td>Returns results in which the property value contains the value you typed anywhere within it. Same as using starting, and ending wildcards.</td>
</tr>
<tr>
<td>Does not contain</td>
<td>Returns results in which the property value does not contain the value you typed anywhere within it.</td>
</tr>
<tr>
<td>Other operators:</td>
<td></td>
</tr>
<tr>
<td>In</td>
<td>Returns results in which the property value matches one of the values you typed. Potential values are typed as a comma-separated list.</td>
</tr>
<tr>
<td>Not in</td>
<td>Returns results in which the property value does not match any of the values you typed.</td>
</tr>
<tr>
<td>Is null</td>
<td>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.</td>
</tr>
<tr>
<td>Is not null</td>
<td>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.</td>
</tr>
</tbody>
</table>

**Viewing 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.

- 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 Monitoring search results in real time, page 496.
• To revise the search, and run it again, click **Edit**, set values, 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 **Saving a search**, page 499.

• 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 **Creating a search template**, page 500.

• To save results from an external source into a repository, see **Saving search results from external sources**, page 497.

### Smart navigation

The smart navigation feature requires that Federated Search Services is installed on Content Server. With smart navigation, results are not only displayed in the content pane, but are also grouped into clusters of related results in the navigation pane. Smart navigation is enabled in the Documentum Administrator preferences, as described in **Setting search preferences**, page 487.

A cluster is created when enough results are available to compute the cluster. As soon as enough results are available, a first set of clusters is displayed. To refresh the **Smart Navigation** list with new results, click ☰. The icon appears when new results are available.

### Monitoring 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 3**, page 497. Search monitoring allows you to see which search sources return results the fastest. Search monitoring is available if the search monitoring Federated 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 3. 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.

**Saving 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. Modify the object properties as many times as needed.

Saved results are available in the selected folder but they are also displayed in My files.

Additional configuration options

The search functionality described 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 can affect your search experience:

- **Indexing**

  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.

- **Relevancy ranking**

  The system administrator can specify a bonus ranking for specific sources, add weight for a specific property value or improve the score for a specific format.

- **Presets**

  The system administrator can define a preset to restrict the list of available types in the Advanced search page. Presets can be different from one repository to another. If you select only external sources, the preset of the current repository applies.

- **Customization of the Advanced search page**

  The Advanced search page can be fully customized to guide you in running queries. For this reason, all the options described in this guide may not be available, and other may appear to narrow and/or condition your queries.

- **Maximum number of results**

  The maximum number of results is defined at two levels. By default, the maximum number of results, taking all sources together, is 1000 and 350 results per source. However, your system administrator can modify these parameters. When querying an external source, the maximum number of results also depends on the configuration set for this source. Results are selected according to their ranking. This way, you always get results with the best ranking; other results are skipped.

- **Case-sensitivity**
If the repository is indexed, queries are case-insensitive by default, even using quotation marks. If the repository is not indexed, then queries are case-sensitive. However, for non-indexed repositories, case-sensitivity can be turned on, and off by the system administrator.

- **Grammatical normalization (lemmatization)**
  When you do not use quotation marks, 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.

## 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: 📚.

## Saving a search

You can save a search so that it can be run again later to retrieve updated results.

### To save a search:

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.
Running 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.

Editing 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 and 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.

Creating a search template

If Federated Search Services is installed on Content Server, Documentum Administrator provides the option to create search templates. A search template is a predefined search in which users can change certain search values each time they run the search. 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:

- ![Public](image) means this search template is public, and accessible to any user.
- ![Private](image) means you are the only one that can access this search template.

Outside of the Saved Searches node, search templates are displayed with a general search icon: ![Search](image).

The *EMC Documentum Federated Search Services Installation Guide* provides more information about installing Federated Search Services.
**To create a search template:**

1. Run an advanced search, 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 sets 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**.
This chapter contains the following topics:

- The Tools menu, page 503
- Lifecycles, page 503
- Workflows, page 505
- Work queue management, page 513
- DQL Editor, page 532
- API Tester, page 532

The Tools menu

API and DQL

DQL queries and server APIs can be run from Documentum Administrator pages that contain a Tools menu. The Use the DQL query pages to run DQL queries and to test whether DQL SELECT statements return the expected values. Use the API pages to enter methods and to send method calls directly to the server.

Lifecycles

A lifecycle defines a sequence of states a file can encounter. Typically, lifecycles are designed for documents to describe a review process. For example, a user creates a document, sends it off to other users for review and approval. The lifecycle defines the state of the file at each point in the process.

The lifecycle itself is created using Documentum Composer and is deployed in the repository as part of an application. Documentum Administrator manages the lifecycles that already exist in a repository. All lifecycle procedures are accessed through the Tools menu in Documentum Administrator.
Assigning a lifecycle to a file

The repository must already contain a lifecycle. You cannot use Documentum Administrator to create a lifecycle.

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, select the lifecycle, the lifecycle state, and an alias set.
   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.

Removing 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.

Promoting 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.

Demoting 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.
Suspending 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.

Resuming 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.

Workflows

A workflow is an automated process that passes files and instructions between individuals in sequence to accomplish specific tasks. When users are assigned a workflow task, the task appears in their 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.

Starting a workflow

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.

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.

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.

**Sending a quickflow**

A quickflow is a single task that is 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.

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.

**Viewing 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 507.

2. To view a specific workflow, select the workflow, then select File > View.

**Pausing 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.


4. If prompted to confirm the pause, click OK.

**Resuming 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.


4. If prompted to confirm, click OK.

**Stopping 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**.

**Emailing 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**.

**Changing 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.

Saving 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.

Viewing 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.
Creating 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.

Configuring the workflow agent

The workflow agent controls the execution of automatic activities in a workflow. The agent is comprised of a master repository session and one or more worker sessions. The master session is dormant until the workflow agent is notified by Content Server that an activity has been created or until the sleep interval expires. At that time, the master session queries the repository for information about the activity or activities and assigns the waiting activity to a free worker session.

Changing the number of worker sessions

The number of worker sessions available to execute automatic activities is controlled by the workflow agent worker threads property value in the server configuration properties. By default, this value is set to 3. You can reset the value to any positive number to a maximum of 1000. Modifying general server configuration information, page 70 provides more information about the server configuration properties.

You must stop and restart Content Server for your change to take effect. Reinitializing the server does not make the change effective.

Changing the sleep interval

The sleep interval determines how long the master session sleeps after querying the repository for activity information in the absence of a notification from Content Server. If the sleep interval expires without a notification, the master session wakes up and queries the repository even though it has not received a notification from Content Server. The default sleep interval is 5 seconds. You cannot change this value in Documentum Administrator. Use IDQL to change the value.

The sleep interval is controlled by the wf_sleep_interval property in the server config object. The value is interpreted in seconds. You must stop and restart Content Server for your change to take effect. Reinitializing the server does not make the change effective.

Changing the system shutdown timeout

The system shutdown timeout property in the server configuration object sets the time that the workflow agent attempts to shut down work items gracefully after receiving a shutdown command. This feature is only applicable for repositories that use multiple Content Servers.

If the shutdown timeout period is exceeded (or is set to zero), the workflow agent shuts down immediately. When the workflow agent does not shut down gracefully, automated tasks in certain
states can be corrupted. If tasks are corrupted, restarting the Content Server does not result in resumption of the managed workflows. The server log file indicates when a graceful shutdown did not occur. Use the RECOVER_AUTO_TASKS administration method to recover the automated tasks.

Note: In some cases, restarting the Content Server after an ungraceful shutdown can result in automated tasks executing again.

If the timeout period is a negative value, Content Server waits for the workflow agent threads to complete the automatic tasks held by workflow agent workers before shutting down gracefully. The default system shutdown timeout setting is 120 seconds. Modifying general server configuration information, page 70 provides more information about the server configuration properties.

Enabling immediate processing of automatic activities

The notify new task attribute (wf_agent_notify_newtask) on the server configuration object enables you to force immediate processing of automatic activities. Configure the Content Server to notify the workflow agent to process automatic tasks immediately after the system creates them by setting the wf_agent_notify_newtask attribute to TRUE. You cannot change this value in Documentum Administrator. Use IDQL to change the value.

When the wf_agent_newtask attribute is set to TRUE, the following occurs:

- If the system creates automatic tasks when the workflow agent is processing the previously collected tasks, then the workflow agent ignores the wf_sleep_interval and collects the next set of automatic activities.
- If the system has not created an automatic task when the workflow agent is processing the previously collected tasks, then the workflow agent sleeps for the time specified in wf_sleep_interval.
- If the system creates tasks when the workflow agent is sleeping, then the agent wakes up immediately and collects the next set of automatic activities.

When the wf_agent_notify_newtask attribute is set to FALSE, the workflow agent honors the value of the wf_sleep_interval and sleeps for the time specified before the workflow agent collects the next set of automatic activities for processing.

By default, the value for the wf_agent_notify_newtask attribute is TRUE.

Tracing the workflow agent

By default, tracing for the workflow agent is turned off. You can turn it on by executing a SET_OPTIONS administration method with the -trace_workflow_agent option specified. SET_OPTIONS, page 261 provides more information about the SET_OPTIONS administration method.

If you execute the SET_OPTIONS administration method, tracing starts immediately. It is not necessary to restart the server. However, if you stop and restart the server, you must reissue the SET_OPTIONS administration method to restart the tracing.

The trace messages are recorded in the server log file.
Disabling the workflow agent

Disabling the workflow agent stops the execution of automatic activities. To disable the workflow agent, set the workflow agent worker threads property in the server configuration properties to 0. Modifying general server configuration information, page 70 provides more information about the server configuration properties.

Stop and restart Content Server for the change to take effect. Reinitializing the server does not make the change effective.

Work queue management

Work queues hold tasks that are to be performed by 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. To access work queues, users must belong to one of the roles described in Table 125, page 513. Work queue users are also referred to as processors.

Apart from work queue users there are

• Work queue managers
  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. Managers can add, edit, and assign skill profiles to individual work queue users.

• Work queue administrators
  Administrator 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 add, edit, or assign skill profiles to the individual work queue users.

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.

Table 125. User roles for work queues

<table>
<thead>
<tr>
<th>Role</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Queue_processor</td>
<td>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.</td>
</tr>
<tr>
<td>Queue_advance_processor</td>
<td>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.</td>
</tr>
<tr>
<td>Role</td>
<td>Description</td>
</tr>
<tr>
<td>----------------------</td>
<td>-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Queue_manager</td>
<td>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.</td>
</tr>
<tr>
<td>Queue_admin</td>
<td>Creates work queues, and queue policies. Members of the queue_admin role do not by default have the administrator role. Queue administrators who have CREATE_GROUP privileges can create work queues.</td>
</tr>
<tr>
<td>Process_report_admin</td>
<td>Runs historical workflow reports from the Workflow menu.</td>
</tr>
</tbody>
</table>

**Setting up a new work queue**

Setting up a work queue requires the following procedures:

- Creating the users, and groups that are used to process the work queues.
- Setting up work assignment matching.
- Creating the queue policies needed for the queue.
- Creating the queue categories.
- Creating the work queue.
- Creating override policies.
- Creating the process templates used for the work queue in Process Builder.

The *EMC Documentum Process Builder User Guide* provides information about defining process templates.

**Setting 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.

Setting 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.

The EMC Documentum Process Builder User Guide: Working with Activities, provides the detailed information.

Defining 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.

**Adding 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.


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 EMC 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.

Creating 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:
2. Navigate to the category where you want to either locate a new policy or edit an existing one.
3. Do one of these:
   - To create a new policy, select File > New > Work Queue Policy.
   - To edit an existing policy, select the policy, and then select View > Properties > Info.
     You may edit the properties of a policy, but the policy name remains a read-only field. To
     rename the policy, you must delete the existing policy, and recreate the same policy with
     the new name.
4. Type a name for the policy.
5. Define these settings:
   - **Threshold**
     The number of unfinished tasks in the queue at which notifications are sent to the queue
     manager warning that the number of tasks in the queue is high. Notifications are triggered
     when the server runs the dm_QmThresholdNotification job.
     The queue managers group is specified in the queue definition, and defines who receives
     the notifications.
   - **Max Priority**
     When a task in the work queue reaches this level, notifications are sent to the queue managers
     group warning that there is an important task not being processed. Notifications are triggered
     when the server runs the dm_QmPriorityNotification job.
   - **Initial Priority**
     The level of importance that is assigned to a newly created task when the work queue uses
     this policy. When a task remains in the queue without being worked on, the system adds
     the number specified in the Increment Priority field to this initial number each time the
     dm_QmPriorityAging job runs.
   - **Increment Priority**
     The value by which the system increments the priority level of tasks that are still in the queue
     each time the system runs the dm_QmPriorityAging job. It is added to the initial priority
     each time that the aging job runs.
   - **Calculate priorities dynamically**
     To use a priority module to set the initial priority, and increase its priority when the aging
     job runs, select the checkbox, and choose a priority module from the list-box. Set dynamic
     priority and aging logic for tasks, page 518 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.

**Defining 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.
   - 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.

**Defining 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. Defining a queue category, page 520, and Work queue policies, page 517 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.

Defining 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:
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.
Managing 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.

Adding 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.

Removing 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.

Adding 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.


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.

Updating 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.
Monitoring 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 Descendants 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.
   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.

**Assigning 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.

**Unassigning 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.
Moving 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 Unassigning a work queue task from a user, page 528.

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.
5. Select the work queue to which to reassign the tasks.
6. Click OK.

Suspending 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.
   
   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.

Unsuspending 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.
   Tip: This action is also available through the Task Manager.

Enabling 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.

Creating 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.
DQL Editor

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.

API Tester

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.


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.
Content Services for SAP Web Administrator

This chapter contains the following topics:

- SAP Web Administrator, page 535
- Configuring Connections to SAP, page 536
- Configuring HTTP Archiving Services, page 537
- The Agent Component, page 540
- Configuring the Manage and View Components, page 547

SAP Web Administrator

Content Services for SAP Web Administrator (WebAdmin) is a browser-based tool hosted within the Documentum Administrator for administering Archive Services for SAP and Content Services for SAP.

The SAP WebAdmin module it is available in Documentum Administrator. The EMC Documentum Content Services for SAP Installation Guide provides the installation information. After Content Services for SAP has been installed, the service appears under the Administration node in Documentum Administrator (Figure 4, page 535).

Figure 4. Content Services for SAP in Documentum Administrator
The Content Services for SAP Web Administration node contains the following subnodes:

- **Actions**: Creates Content Services Actions to perform document linking, data replication, and integrity checking functions.
- **ArchiveLink**: Configures archives, Barcodes for Archive Link, and certificate management.
- **Auto Manage**: Contains the Agent Services for configuring jobs to run the Agent services and monitor the progress of jobs.
- **Clients**: Configures Content Services for the Content Services Manage and Content Services View client applications.
- **Documentum**: Defines Documentum Queries.
- **SAP**: Defines SAP Queries and configure SAP servers and users for Content Services.

## Configuring Connections to SAP

Before you can use Content Services Archive or Agent, you must configure the SAP server and user information. When Content Services for SAP connects to Content Server, it reads the SAP server and user configuration parameters from the repository. The services can be used across multiple SAP application servers.

### Creating, viewing, and editing connections to an SAP server

You must be logged into Documentum Administrator with administrator privileges.

**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** page displays.
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:
   - To log in to an SAP server type the hostname or IP address for the server. When an SAP router is used, enter the complete SAP router string:
     
     /H/router1/H/<host_name_or_IP_address>
   - To log in to an SAP group, which is associated with an SAP R/3 server, select **Enable load balancing**, and type the <SAP_group> in the SAP Logon group field.

   To enable load balancing for SAP server on Windows, add the following entry in the
   
   C:\WINDOWS\system32\drivers\etc\services file on the system that is running the CS
   SAP WebAdmin:
sapms<SID>SID>3600/tcp # SAP System Message Port

Restarting the system is recommended, but not required, to ensure that the changes take effect.

6. Type the system name and number in the appropriate fields.
7. Click OK to save the SAP server configuration.

## Creating, viewing, and editing an SAP user

You must be logged into Documentum Administrator with administrator privileges.

**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 page displays.
   
   **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 page displays.
4. Enter the user name in the New User Name: field.
5. Enter the user ID the User ID: field.
6. Enter a password for the user.
   
   Version 6.0, CS SAP and later 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. Archiving services component has been moved to Archive Services for SAP (AS SAP). The instructions in this section only apply to environment with parallel installations of CS SAP and AS SAP.
SAP must be configured to work with CS SAP. The *EMC Documentum Content Services for SAP Configuration Guide* provides information about configuring SAP using SAPGUI.

## Configuring, viewing, and editing archives

SAP uses named logical archives to specify target storage. Installations typically have a number of archives relating to different types of information.

WebAdmin allows you to specify rules for archived documents/data from SAP, for example storing different types of information in different locations and specifying access permissions, initiate workflows, or define how received documents are rendered into formats such as HTML and PDF.

All configuration objects created in WebAdmin are stored on Content Server. For example, archived information is stored in the /System/DocLink/SAP/Archive folder.

Configuring, viewing, or editing archives requires administrator privileges.

### To configure, view, or edit archives:

1. Connect to WebAdmin.
2. Click to expand the ArchiveLink subnode and select the Archive subnode. The Archive page displays.
3. Select File > New > Archive from the menu at the top of the Archive screen. The Properties page displays.
4. Enter the archive name in the Archive Name: field. The name can have up to 30 character in length for archives.
5. Enter the information on the Properties page, as described in the following table:

### Table 126. Archive properties

<table>
<thead>
<tr>
<th>Fieldname</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Archive ID</td>
<td>A two-letter string that specifies the name of the SAP archive.</td>
</tr>
<tr>
<td>SAP Document Type</td>
<td>The SAP document type. Select NONE (HTTP provided).</td>
</tr>
<tr>
<td>Documentum Type</td>
<td>Specifies the Documentum document type.</td>
</tr>
<tr>
<td>Workflow</td>
<td>Specifies a workflow that is associated with the archive. Select No Workflow.</td>
</tr>
</tbody>
</table>
Fieldname | Description
--- | ---
Attribute Map | Specifies the Documentum attributes of an archived document. The Folder attribute can be configured. By default, the document is stored in the default cabinet. To specify the folder path, use the same format string as for the Agent attribute maps. For example, FOLDER=/SAP/Archive/AA.
Filtering | Specifies filters that are applied during archiving. The following filters are available:
- **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**: Specifies which filters are applied to convert the ALF format into XML for output to PDF, ASCII, or HTML.
- **Service-based business objects (SBO)**: Customize archived object behavior.

The **EMC Documentum Content Services for SAP Administration Guide** provides more information about filtering.

6. Click **OK** to save the archive configuration.

**Configuring HTTP certificates for archive linking**

You must be logged in to Documentum Administrator with administrator privileges.

**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** page displays.
3. Select **File > New > Certificate** from the menu at the top of the **Certificates** screen. The **Certificates Properties** page displays.
4. Right-click on a certificate and select **Properties**. 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.
7. Click OK to save the certificate configuration.

**Configuring HTTP repositories for archive linking**

You must be logged in to Documentum Administrator with administrator privileges.

**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 page displays.
4. Enter the connection information for the repository:
   - **Repository Name:** Name of the repository.
   - **User Name:** User name associated with the repository user.
   - **User Password:** User password associated with the repository user.
   - **Domain:** Domain in which the repository resides.
   Click Test Connection to validate the new repository user access credentials.
5. Enter the connection information for the global repository associated with the repository:
   - **User Name:** User name associated with the global repository user.
   - **User Password:** User password associated with the global repository.
   - **Domain:** Domain in which the global repository resides.
6. Click OK to save the new repository configuration.

**The Agent Component**

The Agent component automates the linking process between SAP objects and documents. 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.

**Note:** The Agent component requires License Key 2 and is not available with License Key 1.

There are three parts to the Agent component known as Actions, Agents, and Jobs (Figure 5, page 541).
Using Auto Manage to execute CS SAP actions

Agents are used to run an action, such as running a job automatically at regular intervals, monitor job progress and job status (Figure 5, page 541).

Figure 5. Agent services

Creating, viewing, and editing an Agent

Agents run actions. Running an action on several servers, requires an Agent for each server. An Agent generates a report file based on a report template. The report template can be edited. The reports are stored in the /System/sysadmin/Reports directory in 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 must be stored in /System/Content Services/DCTM/Template/Report.

Configuring an Agent requires an Action, an SAP Server and SAP user. You must be logged in to Documentum Administrator with administrator privileges.

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. Select the SAP system type from the SAP System Type: drop-down list.
6. Select the action required by the Agent from the Action: drop-down list.
7. Select the SAP server where the Agent is running from the SAP Server: drop-down list.
8. Select 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.
Registering an HVP worker

Registering an HVP worker, requires an Action, an SAP Server, and SAP user. You must be logged in to Documentum Administrator with administrator privileges.

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: page 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:
   http://<host>:<port>/HvpWorker/hvpCommand
6. Select Is Available:.
7. Click OK to save the Worker registration information.

The HVP Worker can be unregistered by disabling the Is Available option on the HVPS properties screen.

Creating, viewing, and editing SAP jobs

A job has two running modes, execute mode and write report mode. When a job is started in execute job mode, the job executes. If the job runs in write report mode, the job only generates a report and does not change any objects. The job also generates a log file containing job specific messages associated with job execution, such as error messages.

You must be logged in to Documentum Administrator with administrator privileges.

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.
The trace level defines the level of detail in the log file. The trace level detail depends on the log level set in the hvp.properties of the HVP Worker. Use hvp.log.level=DEBUG in the hvp.properties file for detailed log.

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 on the Jobs page.

Performing job maintenance

You must be logged in to Documentum Administrator with administrator privileges.

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 on of the following:
   • Properties to make adjustments to the job settings.
   • Run to run the job.
   • Refresh to refresh the Jobs screen.
   • View Job Report to view a job report.
   • View Trace File to view the log file.
   • Delete to delete the job and all its settings

The EMC Documentum System Object Reference Guide provides more information about job status attributes.

SAP queries

SAP queries require at least one SAP user and one SAP server.

Queried SAP objects 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.

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, as described in Table 127, page 545.
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 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. If the query execution on the SAP System takes too long, WebAdmin timeout.

   The window shows the test results and is blank until the query results are returned.

---

**Table 127. Query types**

<table>
<thead>
<tr>
<th>Query types for SAP R/3 version 4.6c</th>
<th>Query types for SAP R/3 version 4.7 and 4.6c</th>
</tr>
</thead>
<tbody>
<tr>
<td>Document info record</td>
<td>No Object PLM (Formerly Document info record)</td>
</tr>
<tr>
<td>Equipment by short text</td>
<td>Equipment by short text PLM</td>
</tr>
<tr>
<td>Functional location by text</td>
<td>Functional location by text PLM</td>
</tr>
<tr>
<td>Material by description</td>
<td>Material by description PLM</td>
</tr>
<tr>
<td></td>
<td><strong>Note:</strong> The Material by description PLM query type has three query conditions:</td>
</tr>
<tr>
<td></td>
<td>• MATERIALSHORTDESCSEL_low</td>
</tr>
<tr>
<td></td>
<td>• MATERIALSHORTDESCSEL_Sign</td>
</tr>
<tr>
<td></td>
<td>• MATERIALSHORTDESCSEL_Option</td>
</tr>
<tr>
<td>Archive data</td>
<td>Archive data</td>
</tr>
<tr>
<td>Cost center</td>
<td>Cost center</td>
</tr>
<tr>
<td>Financial document</td>
<td>Financial document</td>
</tr>
<tr>
<td>Personnel links</td>
<td>Personnel links</td>
</tr>
<tr>
<td>Personnel master</td>
<td>Personnel master</td>
</tr>
<tr>
<td>Purchasing document</td>
<td>Purchasing document</td>
</tr>
<tr>
<td>Customer</td>
<td>Customer Table PLM</td>
</tr>
<tr>
<td>Print list</td>
<td>Print list</td>
</tr>
</tbody>
</table>

---
## Query types for SAP R/3 version 4.6c

<table>
<thead>
<tr>
<th>Vendor</th>
<th>Vendor Table PLM</th>
</tr>
</thead>
<tbody>
<tr>
<td>WBS Element</td>
<td>WBS Element PLM</td>
</tr>
<tr>
<td>Asset Master</td>
<td>Asset Master GetList PLM</td>
</tr>
</tbody>
</table>

## Documentum queries

A Documentum query selects the complete set of linked objects. 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 $ARG expression when defining the DQL statement. For example:
     ```dql
     select r_object_id, object_name from dm_document where object_name = '$ARG1'
     ```
6. Click Execute at the far right of the Query: field.
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.

## Checking the integrity of linked documents

If links are modified or deleted in SAP directories after SAP and Documentum repository objects have been linked, users do not receive any notifications from Content Server. An integrity check action can...
verify whether there are any broken links. The integrity check generates a report that includes any mismatches between the Documentum repository and SAP (Figure 6, page 547).

**Figure 6. Integrity checking**

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 page displays.
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.

**Configuring the Manage and View Components**

The Manage component supports Documentum Administrator’s certified SAP DMS and PLM interfaces. This functionality requires Desktop Client and Documentum Foundation Services (DFS).
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 page displays.

3. Select File > New > Content Services Manage Type Default from the menu at the top of the Content Services Manage Type Defaults page.
   
   The Content Services Manage Type Defaults Properties page displays.

4. Enter the properties information, as described in Table 128, page 548.

5. Click OK to save the Content Services Manage Type Defaults configuration.

### Table 128. Content Services Manage Type Defaults properties

<table>
<thead>
<tr>
<th>Field name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Document Type</td>
<td>Name of the Documentum object type. Enter dm_document to define default settings for all document types.</td>
</tr>
<tr>
<td>SAP Document Type</td>
<td>Specifies the SAP document type that 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.</td>
</tr>
<tr>
<td>Description Attribute</td>
<td>Specifies the name of the property that contains the description value. The default value is object_name.</td>
</tr>
<tr>
<td>Version Label\Required Version</td>
<td>Specifies a set of version labels required for releasing a document to SAP. By default, this feature is turned off when this attribute field is empty.</td>
</tr>
<tr>
<td>Status Label\Required Status</td>
<td>Specifies the status flags that a document must have before it can be released to SAP. By default, this feature is turned off when this attribute field is empty.</td>
</tr>
<tr>
<td>Folder path in Docbase\Required Folder</td>
<td>Specifies one or several folders that the document must be linked to before it can be released to SAP. By default, this feature is turned off when this attribute field is empty.</td>
</tr>
<tr>
<td>Field name</td>
<td>Description</td>
</tr>
<tr>
<td>----------------------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Available Formats\Possible Format</td>
<td>Specifies the set of content types the user can select. These content types must be present in the object when released to SAP. 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.</td>
</tr>
<tr>
<td>Version Label\Possible Version</td>
<td>Specifies the set of versions from which the user can select. These versions must be present in the object when released to SAP. 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.</td>
</tr>
</tbody>
</table>

### 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 page displays.
3. Select File > New > Content Services View from the menu at the top of the Content Services View screen.
   The Content Services View Properties page displays.
4. Enter the properties information, as described in Table 129, page 549.
5. Click OK to save the Content Services View configuration.

#### Table 129. Content Services View properties

<table>
<thead>
<tr>
<th>Field name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Available Formats\Best Formats</td>
<td>Specifies a list of Documentum content types for Best 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.</td>
</tr>
<tr>
<td>Filter Formats</td>
<td>Specifies the formats generated with a Documentum Content Server filter. The formats must be a subset of the formats defined in Best Formats. Each format forces the filter mechanism to generate the required rendition. The filter must be installed on the server.</td>
</tr>
<tr>
<td><strong>Field name</strong></td>
<td><strong>Description</strong></td>
</tr>
<tr>
<td>---------------</td>
<td>----------------</td>
</tr>
<tr>
<td>Standard Attributes\Attributes to Display</td>
<td>The attributes that are used as column header in View’s outline view or are displayed upon request in WebView.</td>
</tr>
<tr>
<td>Force Login</td>
<td>Specifies whether 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.</td>
</tr>
</tbody>
</table>
Chapter 26

My Documentum for Microsoft Outlook Administration

This chapter contains the following topics:
- My Documentum for Microsoft Outlook, page 551
- Overview page, page 552
- Profiles, page 553
- Client Setup, page 557

My Documentum for Microsoft Outlook

My Documentum for Microsoft Outlook is an plug-in to Microsoft Outlook that enables users to work with email messages, associated attachments, and Microsoft Outlook files. Along with the message or file, My Documentum for Microsoft Outlook automatically saves the object properties, such as sender name, recipient names, date, and subject.

Administration tasks for My Documentum for Microsoft Outlook version 6.5 SP1 and later are performed in Documentum Administrator. Many of the configuration settings are stored in the DCO_System_Settings.xml file. This file contains both, server and client environments, and is located in the global repository. For example, the DCO_System_Settings.xml file contains the list of available repositories, object types, and access rights.

Documentum Administrator provides the management and administration of a My Documentum for Microsoft Outlook environment, including profiles, repositories, user configurations, and other options. Repositories must be specifically enabled for use with My Documentum for Microsoft Outlook. A repository is enabled when:

- An administrator navigates to the Profiles folder on the repository for the first time.
- An administrator creates a profile for the first time.
- The repository is added to Repositories section in the dco_custom_settings.xml file in the global repository:

```
<Repositories>
  <Repository name="name of repository" />
</Repositories>
```

Where name of repository is the name of the repository.
Once the My Documentum for Microsoft Outlook applications have been installed on the repository and the settings are enabled under the server.xml Application Server, the **MyDocumentum for Outlook** node appears under the Administration node of the repository (Figure 7, page 552).

**Figure 7. MyDocumentum for Outlook node location in Documentum Administrator**

---

**Overview page**

The Overview link under MyDocumentum for Outlook in Documentum Administrator displays the repository status, and available profiles for all repositories that are configured for My Documentum for Microsoft Outlook(Figure 8, page 553).
Profiles

A profile in My Documentum for Microsoft Outlook is a Documentum object type that defines the user access to repository folder locations, default import settings, and other options. An end-user requires a minimum **Browse** permission to use a particular profile. Users with less than Browse permission cannot see that profile in their Outlook client.

Creating profiles

Use Documentum Administrator to create new profiles on a My Documentum for Microsoft Outlook-enabled repository.

**To create a profile:**

1. Log in to Documentum Administrator with administrator privileges.
2. Click on **My Documentum for Outlook** in the Administration tree.
3. Click **File > New > DCO Profile**.
4. On the **Create** tab, enter the name for the profile in the **Name** field then click **Next**.
5. Enter the information on the **Info** tab, as described in The **Info** tab, page 554.
6. Enter the information on the **Target** tab, as described in The **Target** tab, page 554.
7. Enter the information on **Import** the tab, as described in The **Import** tab, page 554.
8. Enter the information on the **Permissions** tab, as described in The **Permissions** tab, page 556.
The Info tab

To complete the Info tab fields:
1. Enter a description for this profile in the Description field.
2. Specify the profile availability option in the Availability drop-down menu as follows:
   - 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.
3. Specify the default view for users logging into My Documentum for Microsoft Outlook in the The Default View drop-down sets.
   The default views are defined in the Column View node. Users can customize their default view.
   Note: The three default views cannot be deleted.

The Target tab

The Target tab defines which repository folder(s) users can access.

Select the access level in the drop down list of the Give Users Access To field:
- These Folders: Select one or more folders from the list on the left side and click the button to move the folders to the right side. Users can only see folder locations that have been enabled in this profile for My Documentum for Microsoft Outlook, and can only create objects within that folder. If you enable the Users see subfolders option, user have access to all subfolders and can create a subfolders under the target parent folder.
- All Cabinets: Gives users access to all cabinets in the repository.
- Their Home Cabinet: Gives users access to only their home cabinet.
- Their Rooms: Gives users access only to their eRooms.

The Import tab

The Import tab presents configuration options for importing objects into My Documentum for Microsoft Outlook.


Table 130. Import properties

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Property Inheritance</td>
<td>Specifies whether items created in a particular folder inherit keywords and any custom properties that are attached to the folder itself. For example, if one custom folder properties is customer name, any object created in that folder automatically inherits the customer name.</td>
</tr>
<tr>
<td>Provide Dialog Box</td>
<td>Specifies when the user is prompted to complete an import. The options are:</td>
</tr>
<tr>
<td></td>
<td>• <strong>Always</strong>: The user is always prompted to complete the import.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Only if a required field is empty</strong>: The user is only prompted when at least one of the required fields is empty.</td>
</tr>
<tr>
<td>Default settings for Importing Email Messages</td>
<td>Specifies the default message type and permissions set for importing email messages. Select a message type the drop-down list and click Select to select a permission set.</td>
</tr>
<tr>
<td>Default settings for Importing Documents</td>
<td>Specifies the default type and permissions set for importing documents. Select a document type the drop-down list and click Select to select a permission set.</td>
</tr>
<tr>
<td>Default settings for Importing Folders</td>
<td>Specifies the default type and permissions set for importing folders. Select a folder type the drop-down list and click Select to select a permission set.</td>
</tr>
<tr>
<td></td>
<td>The default folder type is dm_folder and the default permission set is NONE, meaning the default permissions for that object type are used.</td>
</tr>
</tbody>
</table>
The Permissions tab

On the Permissions tab you configure access permissions for a profile. User must at least have **Browse** permissions to use the profile and view repository folders in Outlook.

Modifying a profile

**To modify a profile:**

1. Log in to Documentum Administrator with Administrator privileges.
2. Navigate to the **MyDocumentum for Outlook** node under **Administration**.
3. Right-click the highlighted profile name you wish to modify, and select **Properties**.
4. 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 perform an application data sync.

Disabling or deleting a profile can affect the My Documentum for Microsoft Outlook client, as described in **Table 131**, page 556.

<table>
<thead>
<tr>
<th>Client status</th>
<th>Impact</th>
</tr>
</thead>
<tbody>
<tr>
<td>Checked-Out folder contains files</td>
<td>No effect. The client keeps track of checked-out documents and their locations in the repository by unique IDs.</td>
</tr>
<tr>
<td>Documents are in import queue</td>
<td>During full synchronization, documents without synchronization jobs are moved to the <strong>Lost and Found</strong> folder and are not imported. All other synchronization types are no affected.</td>
</tr>
<tr>
<td>Items added to the collisions folder</td>
<td>No effect. The client keeps track of the colliding items and their target locations in the repository by unique IDs.</td>
</tr>
<tr>
<td>during next sync</td>
<td></td>
</tr>
<tr>
<td>Any other items</td>
<td>The client discards any other cached documents, even offline-enabled ones, unless they remain accessible through other profiles.</td>
</tr>
</tbody>
</table>

Deleting profiles

**To delete a profile:**

1. Log in to Documentum Administrator with Administrator privileges.
2. Navigate to the **MyDocumentum for Outlook** node under **Administration**.
3. Click **Profiles**, then Click the name of the profile you wish to delete.
4. Right-click the highlighted profile and select **Delete**. If the profile has more than one version, select whether you want to delete all versions or just the current version.
Deleting a profile does not delete the items in the repository folders. However, users who had previously logged in to My Documentum for Microsoft Outlook using the profile you deleted can no longer access items saved to that profile's location(s) through My Documentum for Microsoft Outlook.

**Client Setup**

On the Client Setup page (Figure 9, page 557), an administrator can control the default options that end users can later modify for their client-side installations.

**Figure 9. The Client Setup page**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
</table>
| Automatic Synchronization | Specifies how often and when content is synchronized while a user is connected to the repository. Valid values are:  
  • **Once a day at ...**: Content is synchronized once a day at the specified time. The time must be entered in 24 hour format.  
  • **Once per hour at ...**: Content is synchronized once per hour at the specified time. The time must be entered in 24 hour format.  
  • **Off**: Content is not synchronized automatically. The user must manually synchronize the content. |

**Table 132. Configuration options for clients**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Email Address for Support</td>
<td>Outlook users can request support from the MyO Outlook Options dialog if you provide an email address.</td>
</tr>
<tr>
<td>Field</td>
<td>Description</td>
</tr>
<tr>
<td>-------------------------------</td>
<td>----------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Sessions Kept in History</td>
<td>Specifies the number of synchronization sessions. End users can view the history of previous synchronization sessions. The <em>EMC Documentum My Documentum for Microsoft Outlook User Guide</em> provides more information on setting end-user preferences and viewing synchronization history on an end-user machine.</td>
</tr>
<tr>
<td>Maximum Disk Space Allowed</td>
<td>Specifies the default value for the maximum storage space allowed on an end-user machine. This value can also be configured on an end-user client machine using the <em>Options</em> dialog box in <em>My Documentum for Microsoft Outlook</em>.</td>
</tr>
<tr>
<td>Email Address for Support</td>
<td>Specifies the email address for technical support requests from end users.</td>
</tr>
</tbody>
</table>
Documentum Reporting Services (DRS) is not integrated with Documentum Administrator. Install DRS to view the DRS Online Help.
AMP and Usage Tracking

This appendix describes the following:

• Asset management and planning tool, page 561
• Connecting to AMP, page 561
• Usage Tracking, page 562

Asset management and planning tool

EMC Asset Management & Planning (AMP) is an enterprise asset management and planning tool that enables users to track and report on the usage of many EMC products. The information in this section is intended to assist system administrators in interpreting the usage tracking information provided by AMP and Content Server.

Usage tracking was introduced in release 6.7. Any Content Server or Documentum application released prior to 6.7 is not tracked by this feature.

Connecting to AMP

AMP collects and displays usage tracking information gathered by the Content Server global registry. EMC recommends that you install AMP to access usage tracking data. AMP provides reports not available with Content Server alone, it allows you to collect usage tracking data from more than one global registry, and it can be configured to work with other EMC products. EMC Documentum Asset Management & Planning (AMP) User Guide provides information on obtaining, installing, and configuring AMP for use with Content Server and other EMC products.

Required information

AMP requires the following information to collect usage tracking information:

• Host-The hostname or IP address of the host machine for the global registry.
• Username-The username to retrieve usage tracking information is dm_report_user.
• Password-The password for the user dm_report_user. At install time, this password is the same password as specified for the user dm_bof_registry.
• JMS Port-The port for the Java Method Server installed for the global registry. The default port number is 9080.
• Global Registry-The name of the repository used as a global registry. This is the repository name specified when the global registry was configured.

Configuring AMP to collect usage information

To use AMP to collect information, create a policy, then schedule the policy to run. When the policy has successfully completed, AMP can display the retrieved data.

To create a policy:
1. Log in to AMP.
2. Select Administration > Policies > Create New.
3. In the Policy Name field, enter a name for the policy.
4. Select Documentum from the Products list.
5. Fill in the information for the Registry Information: Host, Username, Password, JMS Port, and Global Repository.
6. Select Add.
   The Registries box displays the registry information you have entered. Enter additional global registries, if desired.
7. Enter the information for the Scan Frequency and select Save.
8. Select the information arrow icon left of the policy name to run the policy now (if desired). The status bar indicates that policies are running.
   After the policy has completed successfully, view the data by selecting Documentum and viewing the information.

Usage Tracking

When a user logs into Content Server, the system makes an entry in a table managed by Content Server global registry. If this is the first time a user has logged in, a new line is added to the table that records the login name of the user, the name of the application used to log in, and the time of the login. Consequent logins replace the latest use time and the login count in the table.

When a user logs into a Documentum application, that application, in turn, logs into Content Server with the credentials of the user. Therefore, one login to an application that supports usage tracking creates or modifies two lines in the table, one line for the application login and one line for the Content Server login. If you use an application that does not support usage tracking, only the Content Server line is created or modified.
For example, if a user logs in to Webtop, there are two lines modified in the global registry. One line shows the Webtop login and one line shows the Content Server login, since Webtop supports usage tracking. If a user logs in to Content Server using IDQL, there is only one line modified to show the Content Server login, because IDQL does not support usage tracking.

**Tracking internal user accounts**

Content Server creates several user accounts created for internal or system administration purposes. Usage tracking ignores these accounts, when these accounts are used to access Content Server. For example, EMC Asset Management & Planning (AMP) accesses the usage data in the global registry using the account for dm_report_user, and Content Servers connect to the global registry Content Server using the dm_bof_registry user in order to retrieve the common information supplied by the global registry. These users are not recorded when they log in to Content Server. The Content Server installation owner account is also ignored when logging into Content Server.

However, if these accounts are used to log in to an application, the application login is recorded. For example, if the installation owner account is used to log in to Webtop, there is a record of the Webtop login but no record of a Content Server login.

**Tracking unique users**

You can obtain a count of unique users from Content Server, using the dm_usageReport job, or in AMP on the Documentum tab. Depending on your environment, there are cases where you have to verify whether different user login names actually belong to different users or only one user.

When Content Server is set up in domain mode, the user name stored for usage tracking includes the user domain as well as the user login name. For example, user1 in the marketing domain is stored as marketing\user1. If there is a login name user1 in the engineering domain, a login for this user is stored as engineering\user1. When usage tracking or AMP counts unique users, it counts marketing\user1 and engineering\user1 as two distinct users. Depending on your environment, marketing\user1 and engineering\user1 could be the same or two different individuals.

It is also possible that some of the Content Servers using that global registry for usage tracking do not use domain mode, so the user name is stored without a domain. In this case, there can be entries for user1, engineering\user1, and marketing\user1.

You can export the usage tracking data from a global registry if you need to examine the individual entries and verify the unique user counts.

**Tracking login times**

Usage tracking record logins, but it does not provide user tracking in real-time. Usage tracking keeps a cache of previous logins that is retained by each application and Content Server for approximately one day. If a user logs in multiple times in a day, the usage tracking information is typically only
updated once. The purpose of software usage tracking is to provide a long term view of usage without impacting Content Server and application performance.

Specific login times for a user can be obtained from the user object on the Content Server that the user logged into. That particular Content Server is not necessarily the global registry that is used for usage tracking.

**Usage tracking and software compliance**

Usage tracking tracks login information for certain EMC software over time. Software compliance is using the software in conformance with the agreements governing the software license. While the information provided by usage tracking can assist with software compliance, you cannot rely upon it as your only source of compliance information.

Usage tracking reports are provided on an "AS IS" basis for informational purposes only. Inaccuracies can arise due to a number of factors such as inconsistencies in the setup of the global registry, access rights, customizations, availability of usage information within the software asset, and other similar issues. This can result in the collection and reporting of erroneous information. EMC shall not be liable for any errors or omissions in the data, its collection and/or reporting by usage tracking. Regardless of the information provided by usage tracking, customers remain fully liable for utilizing the affected software in full compliance with the authorizing terms and quantities specified in the contract(s), quotes and purchase orders that governed the customer procurement of the software.
Index

A
account
  user, 135
  user privileges, 139
ACL replication job, 189
ACS server
  app.xml file, 117
  configuration object, 118
  connection brokers, 122
  modifying properties, 118
  network location, 116, 120
  projection targets, 120
  properties, 117
  stores, 120
active state
  projecting to connection broker, 82
  repository, 42
  requesting, 42, 81
  server, 81
administration methods, 235
  CAN_FETCH, 237
  CLEAN_LINKS, 238
  DB_STATS, 251
  DELETE_REPLICA, 238
  DESTROY_CONTENT, 239
  DROP_INDEX, 251
  ESTIMATE_SEARCH, 256
  EXEC_SQL, 252
  EXPORT_TICKET_KEY, 240
  FINISH_INDEX_MOVES, 252
  GENERATE_PARTITION_SCHEME_SQL, 253
  GET_LAST_SQL, 258
  GET_PATH, 240
  IMPORT_REPLICA, 241
  IMPORT_TICKET_KEY, 242
  LIST_RESOURCES, 259
  LIST_TARGETS, 260
  MAKE_INDEX, 255
  MARK_FOR_RETRY, 257
  MIGRATE_CONTENT, 242
  MODIFY_TRACE, 258
  MOVE_INDEX, 256
  PURGE_CONTENT, 247
  RECOVER_AUTO_TASKS, 262
  REPLICATE, 248
  RESTORE_CONTENT, 249
  results, 264
  running, 236
  SET_OPTIONS, 261
  SET_STORAGE_STATE, 250
  viewing, 236
  WORKFLOW_AGENT_MANAGEMENT, 263
administrator access sets, 429
Advanced Document Transformation Services, 367
advanced searches, 492
agent
  SAP, 541
  alias, 267
    adding to alias set, 269
  alias set, 267
    adding aliases, 269
    creating, 267
    deleting, 270
    of a user, 147
AMP, 561
API, 503
  running, 532
app.xml file, 117
application servers
  creating, 77
  modifying, 77
  server configuration object, 77
archiving, content files, 192
arguments
  recovery_publish_retry_count, 347
  set_tcp_delay, 348
  store_log_file, 343
assembling virtual documents, 473
assignment policies, 281, 317
rule execution, 317
triggers, 317
assignment policy
creating, 319
custom rules, 321
deleting, 322
modifying, 319
asynchronous write job, 189
Atmos stores, 308
creating, 308
Audio/Video Transformation Services, 367
audit
policies, 181
audit events
in workflows, 507
audit management job, 189
audit policy
modifying, 182
properties, 182
audit trails
deleting, 184
displaying, 184
searching, 180
viewing, 180
auditing, 175
all objects, 179
events, 179
modifying, 184
object instances, 178
object type, 176
selection criteria, 183
audits
registering, 183
authentication
Kerberos with LDAP, 109
LDAP, 100
authentication failure, resource agents, 419
automatic activities
execution
configuring, 511
disabling, 513
automatic tasks
in workflows, 505

B

BAPI, 544
binding password, LDAP server, 107
blob stores
creating, 294
distributed stores, 294
properties, 294
BOCS
job, 220
job caching rules, 220
BOCS server, 123
communication protocols, 127
configuration object, 124
Consume URL, 130
creating, 124
encryption, 128
message routing, 130
network location, 116
Post URL, 130
pre-caching, 128
public key, 126
pull mode, 126
push mode, 126
security properties, 126
BOCS servers
deleting, 128
bookmarks
adding repository document or folder, 466
subscriptions, 467
Branch Office Caching Services (BOCS), 123
Business Process Manager, 85

C
cabinet
creating, 455
cached types
modifying, 78
server configuration object, 78
Calendars, 441
CAN_FETCH administration method, 237
categories
copying, 463
deleting, 467
link to multiple locations, 465
search, 492
work queue categories, 520, 527
checkin
generate versions, 461
checking out
files, 459
checkout
canceling, 461
view files, 461
child documents
   in virtual documents, 471
CIS, 377
   bring taxonomies online, 401
category classes, 392
category rules, 389
clearing analysis results, 414
clearing assignments, 414
configuration settings, 381
creating document sets, 406
creating taxonomies, 384, 394
defining categories, 395
deleting taxonomies, 404
enabling repository, 380
property rules, 397
reviewing documents, 413
submitting a document set, 410
submitting one document, 410
synchronizing taxonomies, 400
testing, 412
CLEAN_LINKS administration
   method, 238
client applications
   virtual document components,
      obtaining path to, 479
client rights domain, 433
   adding, 434
deleting, 434
   enabling or disabling, 434
   member repository, 435
clipboard
   adding to, 467
   removing from, 467
   viewing, 467
code pages
   dump and load requirements, 45
communication protocol
   BOCS server, 127
confidence values, 388
configuration
   repository, 34
   configuring process engine, 85
connection broker
   log file, 83
   session, 31
connection brokers
   ACS server, 122
LIST_TARGETS administration
   method, 260
   server configuration object, 75
consistency checker job, 190
Consistency Checker tool, 59
   report sample, 60
consistency_checker.ebs, 59
content
   in virtual document, 473
   method, 234
content caching
   job, 220
content delivery
   deleting logs, 357
   logs, viewing, 357
   publishing objects, 355
content delivery configuration, 329
   advanced properties, 333
deactivating, 354
deleting, 353
duplicating configurations, 354
   extra arguments, 339
ingesting content, 356
   replication properties, 338
   results, 356
testing, 353
content delivery configurations
   creating, 331
   locating, 330
content file cleanup, 193
content files
   archiving, 192
   without content objects, 193
content files, moving, 215
Content Intelligence Services
   introduction, 377
   setting up, 379
content methods, 236
   CAN_FETCH administration
      method, 237
content migration job
   creating, 322
   rules, 324
   schedule, 324
   SysObject information, 326
content migration jobs, 322
content objects, orphaned, 192
content replication job, 191
Content Server
   multiple with LDAP, 108
roles, 155
server log file, 83
Content Services for EMC Centera
(CSEC), 300
Content Services for SAP Archive, 536
Content Transformation Services, 367
content warning job, 191
creating
file stores, 288
locations, 78
criteria, auditing, 183
CSEC, 300
CTS
administration, 367
changing the logging interval, 369
changing the maximum number of
queue items, 370
changing the notification setting, 370
changing the polling interval, 368
changing the queue item expiry, 371
changing the system operator, 369
changing user for an instance, 367
configuring an instance, 368
controlling instance, 372
log files, 369, 371
products, 367
refreshing a service, 373
starting a service, 373
stopping a service, 372
viewing a log file, 371
viewing instance details, 372

D
data dictionary publisher job, 191
database methods, 236
database space warning job, 192
databases, statistics, 251
date values, 45
DB_STATS administration method, 251
default renditions
setting, 470
DELETE_REPLICA administration
method, 238
deleting
groups, 154
users, 145
users from group, 154
descendants
in virtual documents, 471
DESTROY_CONTENT administration
method, 239
details
workflows, 507
DFC
privileged clients, 437
dfc.properties file
enabling global repository, 43
disabling
save, 81
disk capacity, 191
distributed configurations, 113
distributed content
configuring object, 128
distributed operations job, 192
distributed repositories
distributed operations job, 192
distributed storage, content
replication, 191
distributed stores, 295
blob stores, 294
creating, 296
modifying, 296
replicating objects, 208
distributed transfer
ACS read setting, 128
ACS write setting, 128
BOCS pre-caching, 128
dm_ACLRepl_job, 189
dm_ACLReplication job, 189
dm_AsyncronousWrite_job, 189
dm_AuditMgt job, 189
dm_AccessManager job, 189
dm_AccessManager job, 189
dm_Auditor job, 189
dm_AuditMgt job, 189
dm_AuditMgt job, 189
dm_AuditMgt job, 189
...
Index

dm_GroupRename job, 194
dm_LDAPSynchronization job, 195
dm_load_record, 46
dm_LogPurge job, 196
dm_QueueMgt job, 196
dm_RemoveExpiredRetnObjects job, 197
dm_RenditionMgt job, 198
dm_report_user, 199
dm_SCSLogPurgeJob job, 198
dm_StateOfDocbase job, 198
dm_SwapInfo job, 199
dm_UpdateStats job, 199
dm_usage_log, 199
dm_UserChgHomeDb job, 200
dm_UserRename job, 200
dm_VersionMgt job, 201
dm_WfmsTimer job, 201, 454
dmclean job, 192
dmfilesan job, 193
dmi_dump_object_record, 46
dmi_load_object_record, 46
DMS
configuration, 130
docbase config object, 33
Docbasic, 205, 228
document confidence scores, 388
Document Transformation Services, 367
documents
publishing, 355
transforming to HTML, 470
transforming to PDF, 470
Documentum Administrator
connecting to, 25
version, 29
Documentum Offline Client
repository synchronization, 40
Documentum Site Caching Services,
logs, 198
domain authentication, 65
domain controllers, 66
domain maps, 65
domains, 66
dormant state
projecting to connection broker, 82
repository, 41
requesting, 41, 80
server, 80
DQL queries, 503
running, 532
DROP_INDEX administration method, 251
dump files, compatibility issues, 45
dump object record, 46
dump record object, 46
dumping
repositories, 45
sample script, 51
dynamic group, 149

E
electronic signature
BOCS server, 126
e-mail messages
sending links, 467
EMC Centera store
storage parameters, 303
EMC Centera stores
creating, 301, 305
enabling
save, 81
encryption
BOCS server, 128
escalated privileges, 437
ESTIMATE_SEARCH administration
method, 256
events
auditing, 179
evidence
reusing, 392
evidence propagation, 392
EXEC_SQL administration method, 252
EXPORT_TICKET_KEY administration
method, 240
external stores
creating, 298
limitations, 297
plug-ins, 297

F
failover
LDAP server properties, 103
far stores
modifying, 79
server configuration object, 79
favorites
adding repository document or
folder, 466
federated security mode, 214
federation
adding members, 88
deleting, 88
deleting members, 88
federation copy job, 193
federation export job, 193
federation import job, 193
federation status job, 194
federation update job, 194
federations, 85
connection broker information, 86
jobs, 193
users, 140
file formats, 271
file report jobs, 194
file stores
creating, 288
files
canceling checkout, 461
checking in, 459
checking out, 459
copying, 463
copying locally, 464
creating, 457
deleting, 467
demoting, 504
edit, 459
exporting, 464
importing, 463
lifecycles, 504
link to multiple locations, 465
linking to other repositories, 465
removing lifecycles, 504
renditions, 469
sending to workflows, 505
unlocking, 461
versions, 461
viewing, 463
viewing locations, 466
virtual links, 463
filters
in work queues, 515 to 516
FINISH_INDEX_MOVES administration method, 252
folders
copying, 463
creating, 457
deleting, 467
link to multiple locations, 465
viewing locations, 466
format
creating, 271
deleting, 273
modifying, 271
forms
creating, 458
full-text indexes
estimating results, 256
marking content files, 257
tracing, 258
full-text indexing
administration methods, 235
creating queue items, 364
index agents, 359
queue items, 362, 364
xPlore, 359
xPlore installations, 359
full-text indexing methods, 237
G
GENERATE_PARTITION_SCHEMA_SQL administration method, 253
GET_LAST_SQL administration method, 258
GET_PATH administration method, 240
global registries
network locations, 113 to 114
global registry, 42
in client rights domain, 433
global user
creating, 140
global users, 85
group
adding to a work queue, 523
adding users, 153
deleting, 154
dynamic, 149
locating, 151
removing users, 154
viewing where used, 151
group rename job, 194
groups, 133, 148
federations, 193
of a user, 147
privileged, 149
reassigning, 154
H
highlights
  in search results, 495
historical reports
  workflows, 510
home repository, 146

I
import file
  user, 144
IMPORT_REPLICA administration
  method, 241
IMPORT_TICKET_KEY administration
  method, 242
importing
  users, 141
Inbox
  availability options, 484
index agents, 359
  disabled, 360
  enabling, 361
  modifying properties, 361
  properties, 361
  starting, 360
  stopping, 360
indexes
  creating, 255
  destroying, 251
  moving, 252 to 253, 256
Interactive Delivery Services, 329
  effective labels, 358
Interactive Delivery Services Accelerated, IDSx, 329
internationalization
  dump and load requirements, 45

J
Java method server, 90
  active, 93
  associated Content Servers, 92
  cache, 93
  configuration object, 90 to 91
  failover, 90
  modifying configuration, 91
  properties, 91
  status, 93
  URL, 91
Java methods, 228
JMS, 90
JMX Service URL, 418 to 419
job
  BOCS, 220
  BOCS caching rules, 220
  changing schedule, 203
  content migration jobs, 322
  creating sequences, 222
  deactivating on failure, 227
  deleting, 227
  dm_ACLRepl, 189
  dm_ACLReplication, 189
  dm_AsyncWrite, 189
  dm_AuditMgt, 189
  dm_ConsistencyChecker, 190
  dm_ContentReplication, 191
  dm_DataDictionaryPublisher, 191
  dm_DBWarning, 192
  dm_DistOperations, 192
  dm_DMArchive, 192
  dm_DMclean, 192
  dm_DMfilescan, 193
  dm_FederationCopy, 193
  dm_FederationExport, 193
  dm_FederationStatus, 194
  dm_FederationUpdate, 194
  dm_FileReport, 194
  dm_GroupRename, 194
  dm_LDAPSynchronization, 195
  dm_LogPurge, 196
  dm_QueueMgt, 196
  dm_RemoveExpiredRetnObjects, 197
  dm_RenditionMgt, 198
  dm_StateOfDocbase, 198
  dm_SwapInfo, 199
  dm_UpdateStats, 199
  dm_UserChgHomeDb, 200
  dm_UserRename, 200
  dm_VersionMgt, 201
  dm_WfmsTimer, 201
  dmFederationImport, 193
  locating method, 207
  method, 205
  method properties, 206
  properties, 202, 204
  qualifier rules, 204
  records migration, 215
  remove expired retention objects, 219
  replication, 208
  running, 225
SCSLogPurgeJob, 198
sysobject properties, 207
trace levels, 226
trace logs, 227
viewing reports, 226
viewing status, 226
job sequence
dependencies, 225
select jobs, 224
job sequences
choosing repositories, 223
jobs, 187
creating, 201
default, 187
dm_ConistencyChecker, 59
dm_ContentWarning, 191

K
Kerberos
LDAP synchronization, 109

L
LDAP
jobs, 195
synchronization, 195
LDAP certificates
importing, 110
replacing, 111
LDAP server, 94
attribute map, 105
binding password, 107
certificate properties, 110
configuration object, 95
deleting object, 108
duplicate configuration object, 107
failover, 103
Kerberos users, 109
LDAP directory, 97
mapping, 101, 104 to 105
modifying configuration, 96
multiple Content Servers, 108
multiple servers, 111
properties, 95, 97
proxy server support, 109
secondary, 106
secure connection information, 97
synchronization, 100, 107
user authentication, 100
LDAP synchronization job, 195
ldap<objectID>.cnt file, 97
LDIF file formats, 141
licensure
  Rentention Policy Services, 32
license
  Federated Record Services, 32
  managing, 32
  Physical Records Management, 32
  Records Manager, 32
license, Collaboration Edition, 32
lifecycles, 503
  assigning, 504
  demoting, 504
  promoting, 504
  removing, 504
  resuming, 505
  suspending, 505
lightweight object type
  conversion to, 282
linked stores
  creating, 293
links
  common tasks, 465
  deleting, 467
  in email messages, 467
  subscriptions, 467
  to multiple locations, 465
  to other repositories, 465
  viewing locations of, 466
Linux
  Windows domain authentication, 65
to 66
LIST_RESOURCES administration
  method, 259
LIST_TARGETS administration
  method, 260
loading
  compatibility issues, 45
  repositories, 45
locating
  groups, 151
  job method, 207
location object
  creating, 313
  modifying, 313
  properties, 313
location objects, 312
file stores, 288
locations
deleting, 315
modifying, 78
server configuration object, 78
viewing, 466
locked files
view, 461
viewing, 463
log
job trace, 227
log files
storing, 343
log purge job, 196
logs
content delivery, 357
purging, 196
Site Caching Services, 198
user reassign, 147

M
MAKE_INDEX administration method, 255
mapping
LDAP server, 101, 104
mapping, LDAP server, 105
MARK_FOR_RETRY administration method, 257
MBean resources, 420
Media Transformation Services, 367
Medical Imaging Transformation Services, 367
messaging server
configuration object, 130
messaging servers
 copying, 131
method
 execution, 205
 jobs, 201
 locating job, 207
methods, 228
 checking in content, 234
 creating, 228
 deleting, 235
 exporting content, 233
 importing content, 231
 modifying, 228
 modifying content, 234
 running, 232
 storing content, 228
 storing executable program, 228
viewing results, 233
MIGRATE_CONTENT administration method, 242
migration policy
deleting, 327
MODIFY_TRACE administration method, 258
modifying
locations, 78
module role
creating, 159
deleting, 160
properties, 159
reassigning, 160
module roles, 158
mount point
creating, 311
properties, 311
mount point object, 311
mount points
deleting, 315
MOVE_INDEX administration method, 256
My Documentum for Microsoft Outlook, 551
client setup, 557
creating profiles, 553
profile import preferences, 554
profile target settings, 554
profiles, 553
My Files
view, 461

N
NetApp SnapLock store
creating, 306
properties, 306
NetApp SnapLock stores, 305
network location
ACS server, 120
network locations, 113
copying, 115
creating, 114
deleting, 116
global registries, 113 to 114
properties, 114
server configuration object, 76
non-federated security mode, 214
O

object
  alias set, 267
  auditing properties, 176, 183
  BOCS configuration, 124
  distributed transfer, 128
  file, 271
  instance auditing properties, 178
  LDAP configuration, 97
  messaging server configuration, 130
  reindex failed, 363
  relationships, 468
  resubmitting for indexing, 363
  server configuration, 67
  user configuration, 135

object instance
  auditing, 178

object type
  converting to lightweight, 282
  converting to shareable, 281
  converting to shareable and lightweight, 283
  creating, 276
  deleting, 280
  modifying, 276
  selecting, 280

object types
  auditing, 176

objects
  dump object record, 46
  dump record, 46
  operating system information, 259
  Oracle, 192
  orphaned content objects, 192

P

parent documents
  of virtual documents, 471
path_name property, 479
PDF documents, 471
  configuring annotation services, 471
permission
  properties, 166
permission set
  adding users, 170
  creating, 166
  deleting, 171
  deleting users, 171
  permissions, 167

properties, 166
validations, 166
viewing associations, 173

permission sets, 165
locating, 165
replica objects, 213
validating, 174

permissions
  changing, 173
  of a user, 147
  viewing associations, 173

plug-in
  creating, 314
  modifying, 314
  properties, 315

plug-ins, 314
  Content Services for EMC Centera (CSEC), 301
deleting, 315
  EMC Centera stores, 300
  external stores, 297
  NetApp SnapLock stores, 305

preferences
  searches, 487
  virtual documents, 477

privileged DFC
  role groups used by, 150
privileged DFC clients, 437
privileged groups, 149
  role groups used by DFC, 150

process engine
  disabling, 85
process template, 515
profiles
  creating in My Documentum for Microsoft Outlook, 553
  My Documentum for Microsoft Outlook, 553

Profiles
  My Documentum for Microsoft Outlook import, 554

projecting to connection broker
  active state, 82
dormant state, 82
projection targets
  creating, 75 to 76
deleting, 75 to 76
modifying, 75 to 76

properties
ACS server, 118
audit policies, 182
blob store, 294
BOCS server, 124
dump record object, 46
Java method server, 91
job, 202
job method, 206
job schedule, 204
LDAP authentication, 100
LDAP certificate, 110
LDAP server, 97
LDAP server failover, 103
LDAP server mapping, 101
location object, 313
module roles, 159
mount point, 311
network locations, 114
object auditing, 176
object instance auditing, 178
permission, 167
permission set, 166
plug-in, 315
roles, 155
secondary LDAP server, 106
server configuration object, 68
sessions, 161
user account, 135

proxy server
LDAP, 109
public key certificate, 437
publishing documents
by date, 358
effective label, 358
publishing objects, 355
PURGE_CONTENT administration method, 247

Q
queries
search queries, 496
queue items, 362
indexing status, 362
queue items, indexing
creating, 364
removing by status, 363
removing individual, 364
viewing, 364
queue management job, 196
queue policies, 515
queue processors
enabling selective pull, 530
managing, 523
quickflows
sending, 507

R
reassigning
groups, 154
records migration job
creating, 215
rules, 216
selection criteria, 217
version criteria, 218
RECOVER_AUTO_TASKS administration method, 262
recovering from failed publish, 347
recovery_publish_retry_count, 347
refreshing
a CTS service, 373
related items
deleting, 467
relationships
creating, 468
deleting, 469
removing, 469
viewing, 468
remove expired retention objects job
creating, 219
rendition manager job, 198
renditions
deleting, 198
importing, 469
overview, 469
setting a default, 470
viewing, 469
replica objects
permission set, 213
REPLICATE administration method, 248
replication
job, 208
SAP to Documentum repository, 540
replication job
options, 210
source repository, 209
<table>
<thead>
<tr>
<th>Index</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>target repository, 209</td>
<td>resource management, 417</td>
</tr>
<tr>
<td>replication jobs</td>
<td>Resource Management</td>
</tr>
<tr>
<td>creating, 208</td>
<td>resource agents, managing, 417</td>
</tr>
<tr>
<td>security mode, 213</td>
<td>RESTORE_CONTENT administration</td>
</tr>
<tr>
<td>storage areas, 213</td>
<td>method, 249</td>
</tr>
<tr>
<td>reports</td>
<td>results</td>
</tr>
<tr>
<td>job, 226</td>
<td>external sources, 497</td>
</tr>
<tr>
<td>workflows, 510</td>
<td>searches, 495 to 496</td>
</tr>
<tr>
<td>repositories, 33</td>
<td>retention date, 316</td>
</tr>
<tr>
<td>adding to a federation, 88</td>
<td>retention store</td>
</tr>
<tr>
<td>dump and load compatibility issues, 45</td>
<td>EMC Centera, 300</td>
</tr>
<tr>
<td>dumping and loading, 45</td>
<td>reviews</td>
</tr>
<tr>
<td>duplicating, 45</td>
<td>quickflows, 507</td>
</tr>
<tr>
<td>federations, 85</td>
<td>role</td>
</tr>
<tr>
<td>groups, 148</td>
<td>adding groups, 157</td>
</tr>
<tr>
<td>job sequences, 223</td>
<td>adding roles, 157</td>
</tr>
<tr>
<td>moving, 45</td>
<td>adding users, 157</td>
</tr>
<tr>
<td>removing a federation, 88</td>
<td>creating, 155</td>
</tr>
<tr>
<td>sample dump script, 51</td>
<td>deleting, 158</td>
</tr>
<tr>
<td>users, 134</td>
<td>properties, 155</td>
</tr>
<tr>
<td>repository</td>
<td>reassigning, 158</td>
</tr>
<tr>
<td>active state, 42</td>
<td>roles, 133, 155</td>
</tr>
<tr>
<td>cleaning, 57</td>
<td>in work queues, 513</td>
</tr>
<tr>
<td>date and time values, 45</td>
<td>roles, for privileged DFC, 150</td>
</tr>
<tr>
<td>dormant state, 41</td>
<td>rules</td>
</tr>
<tr>
<td>enabling for CIS, 380</td>
<td>job, 204</td>
</tr>
<tr>
<td>enabling global registry, 42</td>
<td>record migration job, 216</td>
</tr>
<tr>
<td>in client rights domain, 433</td>
<td></td>
</tr>
<tr>
<td>session, 161</td>
<td></td>
</tr>
<tr>
<td>synchronization, 40</td>
<td></td>
</tr>
<tr>
<td>repository configuration</td>
<td></td>
</tr>
<tr>
<td>modifying, 34</td>
<td></td>
</tr>
<tr>
<td>Resource Agent Authentication page, 419</td>
<td></td>
</tr>
<tr>
<td>resource agent resources</td>
<td></td>
</tr>
<tr>
<td>attributes, 421</td>
<td></td>
</tr>
<tr>
<td>general information, 421</td>
<td></td>
</tr>
<tr>
<td>log file, 424</td>
<td></td>
</tr>
<tr>
<td>managing, 420</td>
<td></td>
</tr>
<tr>
<td>notifications, 423 to 424</td>
<td></td>
</tr>
<tr>
<td>operations, 422</td>
<td></td>
</tr>
<tr>
<td>starting operations, 423</td>
<td></td>
</tr>
<tr>
<td>resource agents</td>
<td></td>
</tr>
<tr>
<td>adding, 418</td>
<td></td>
</tr>
<tr>
<td>authentication failure, 419</td>
<td></td>
</tr>
<tr>
<td>deleting, 419</td>
<td></td>
</tr>
<tr>
<td>managing, 417</td>
<td></td>
</tr>
<tr>
<td>properties, 419</td>
<td></td>
</tr>
<tr>
<td>resources, 420</td>
<td></td>
</tr>
<tr>
<td>resource logs</td>
<td></td>
</tr>
<tr>
<td>resource agent resources, 424</td>
<td></td>
</tr>
<tr>
<td>Resource Agent Authentication page, 419</td>
<td></td>
</tr>
<tr>
<td>resource agent resources</td>
<td></td>
</tr>
<tr>
<td>attributes, 421</td>
<td></td>
</tr>
<tr>
<td>general information, 421</td>
<td></td>
</tr>
<tr>
<td>log file, 424</td>
<td></td>
</tr>
<tr>
<td>managing, 420</td>
<td></td>
</tr>
<tr>
<td>notifications, 423 to 424</td>
<td></td>
</tr>
<tr>
<td>operations, 422</td>
<td></td>
</tr>
<tr>
<td>starting operations, 423</td>
<td></td>
</tr>
<tr>
<td>resource agents</td>
<td></td>
</tr>
<tr>
<td>adding, 418</td>
<td></td>
</tr>
<tr>
<td>authentication failure, 419</td>
<td></td>
</tr>
<tr>
<td>deleting, 419</td>
<td></td>
</tr>
<tr>
<td>managing, 417</td>
<td></td>
</tr>
<tr>
<td>properties, 419</td>
<td></td>
</tr>
<tr>
<td>resources, 420</td>
<td></td>
</tr>
<tr>
<td>resource logs</td>
<td></td>
</tr>
<tr>
<td>resource agent resources, 424</td>
<td></td>
</tr>
</tbody>
</table>
searches
  advanced searches, 492
  configuration, 498
  edit, 492, 500
  external results, 497
  highlight results, 495
  monitor, 495 to 496
  operators, 489
  preferences, 487
  results, 495 to 496
  saved searches, 499 to 500
  simple searches, 489
  status, 495 to 496

security
  auditing, 175
  BOCS server, 126
  replication job, 213

security mode
  federated, 214
  non-federated, 214

SELECT (statement)
  processing algorithm, 474

selection criteria
  records migration job, 217

sequences
  job, 222

server
  active state, 81
  dormant state, 80

server configuration object, 67
  application servers, 77
  Business Process Manager, 85
  cached types, 78
  connection brokers, 75
  creating, 68, 70
  deleting, 84
  disabling process engine, 85
  duplicating, 69
  far stores, 79
  info properties, 70
  locations, 78
  modifying, 68
  network locations, 76
  process engine, 85
  projection targets, 75

server root location
  modifying, 299

serverlog file, 83

servers
  server configuration object, 67

session
  info, 161
  killing, 163
  logs, 162
  viewing, 161
  sessions, 161
  user, 133

SET_OPTIONS administration
  method, 261

SET_STORAGE_STATE administration
  method, 250

set_tcp_delay, 348

shareable object type
  conversion to, 281

shortcuts
  links, 465
  subscriptions, 467
  to items in other repositories, 465

showing all, 134

simple search
  run, 489

simple searches
  run, 489

sleep interval (workflow agent)
  changing, 511

snapshots
  creating, 476
  path_name property, 479

source host log files, 343

SQL Server, 192

SQL statements, 252

SSL mode, 111

starting
  a CTS service, 373
  State of Repository job, 198
  stemming, 390

stopping
  a CTS service, 372

storage, 285
  blob stores, 294
  deleting, 315
  distributed stores, 295
  EMC Centera stores, 300 to 301, 305
  external stores, 297 to 299
  file stores, 288
  linked stores, 293
  NetApp SnapLock stores, 305

storage areas
  migrating records, 215
  moving content, 322
storage policies, 317
store_log_file, 343
stores
  ACS server, 120
  Atmos, 308
structure
  of virtual document, 472
subscriptions
  creating, 467
  viewing, 467
swap info job, 199
synchronization
  LDAP server, 100
system information, 27

T
  tasks
    completing, 482
    performing, 482
    reassigning, 484
taxonomy
  online, 401
trace levels
  setting, 226
trace log
  jobs, 227
trace methods, 237
tracking
  login times, 563
  software usage, 561
troubleshooting
  server, 83

U

Update Statistics job, 199
usage tracking, 199, 561
user
  adding to a work queue, 523
  adding to permission sets, 166, 170
  changing home repository, 146
  changing permissions, 173
  changing state, 146
  configuration object, 135
  creating, 135
  deleting, 145
  deleting from permission sets, 171
documents, 147
global, 140
groups, 147
importing, 141
LDFI file formats, 141
login domain, 136
login name, 136
permission sets, 147
privileges, 139
properties, 135
reassign logs, 147
reassigning, 145
session info, 161
sessions, 161
user change home repository job, 200
user management, 133 to 134
user rename job, 200
user source property, 137
users
  adding to a group, 153
  alias sets, 147
  assigning tasks, 528
  changing for a CTS instance, 367
  federations, 85
global, 85
  locating, 134
  sessions, 133
  workflows, 147
validating
  permission sets, 174
vdmPath method, 479
vdmPathDQL method, 479
version criteria
  records migration job, 218
version management job, 201
versions
  deleting, 467
  renditioning, 469
  save new, 459
  view, 461
viewing
  job trace logs, 227
virtual documents, 471
  archiving, 475
  assembling, 473
components
  appending, 472
  determining paths to, 479
content, 473
<table>
<thead>
<tr>
<th>Index</th>
</tr>
</thead>
<tbody>
<tr>
<td>converting to simple documents, 476</td>
</tr>
<tr>
<td>creating, 471 to 472</td>
</tr>
<tr>
<td>freezing snapshots, 476</td>
</tr>
<tr>
<td>preferences, 477</td>
</tr>
<tr>
<td>querying, 478</td>
</tr>
<tr>
<td>snapshots, 475</td>
</tr>
<tr>
<td>creating, 476</td>
</tr>
<tr>
<td>structure, 472</td>
</tr>
<tr>
<td>unfreezing snapshots, 476</td>
</tr>
<tr>
<td>vdmPath method, 479</td>
</tr>
<tr>
<td>vdmPathDQL method, 479</td>
</tr>
<tr>
<td>version labels, 475</td>
</tr>
<tr>
<td>policies, 517</td>
</tr>
<tr>
<td>reassigning tasks, 529</td>
</tr>
<tr>
<td>removing group, 524</td>
</tr>
<tr>
<td>removing user, 524</td>
</tr>
<tr>
<td>resuming suspended tasks, 529</td>
</tr>
<tr>
<td>roles, 513</td>
</tr>
<tr>
<td>suspending tasks, 529</td>
</tr>
<tr>
<td>unassigning tasks, 528</td>
</tr>
<tr>
<td>worker sessions (workflow agent)</td>
</tr>
<tr>
<td>changing number of, 511</td>
</tr>
<tr>
<td>workflow</td>
</tr>
<tr>
<td>RECOVER_AUTO_TASKS, 262</td>
</tr>
<tr>
<td>WORKFLOW_AGENT_MANAGEMENT, 263</td>
</tr>
<tr>
<td>workflow agent</td>
</tr>
<tr>
<td>configuring, 511</td>
</tr>
<tr>
<td>disabling, 513</td>
</tr>
<tr>
<td>sleep interval, changing, 511</td>
</tr>
<tr>
<td>tracing, 512</td>
</tr>
<tr>
<td>worker sessions, changing number, 511</td>
</tr>
<tr>
<td>workflow methods, 237</td>
</tr>
<tr>
<td>WORKFLOW_AGENT_MANAGEMENT administration method, 263</td>
</tr>
<tr>
<td>workflows</td>
</tr>
<tr>
<td>audit events, 507</td>
</tr>
<tr>
<td>changing supervisor, 509</td>
</tr>
<tr>
<td>completing failed tasks, 509</td>
</tr>
<tr>
<td>completing tasks, 482</td>
</tr>
<tr>
<td>creating templates, 511</td>
</tr>
<tr>
<td>details, 507</td>
</tr>
<tr>
<td>emailing participants, 509</td>
</tr>
<tr>
<td>failed tasks, 509</td>
</tr>
<tr>
<td>of a user, 147</td>
</tr>
<tr>
<td>pausing, 508</td>
</tr>
<tr>
<td>rejecting tasks, 483</td>
</tr>
<tr>
<td>reports, 510</td>
</tr>
<tr>
<td>resuming, 508</td>
</tr>
<tr>
<td>starting, 505</td>
</tr>
<tr>
<td>stopping, 508</td>
</tr>
<tr>
<td>viewing, 507</td>
</tr>
<tr>
<td>workflow agent, 511</td>
</tr>
<tr>
<td>X</td>
</tr>
<tr>
<td>XML store, creating, 298</td>
</tr>
<tr>
<td>xPlore, 359</td>
</tr>
<tr>
<td>xPlore installations, 359</td>
</tr>
</tbody>
</table>