

## OpenText™ Documentum™ Content Management

### **Administrator User Guide**

Manage repositories, connection brokers, users and groups, storage areas, and security using the OpenText Documentum Content Management (CM) Administrator graphical user interface.

EDCAC250400-UGD-EN-01

---

## **OpenText™ Documentum™ Content Management**

### **Administrator User Guide**

EDCAC250400-UGD-EN-01

Rev.: 2025-Nov-18

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

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

#### **Open Text Corporation**

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

Tel: +1-519-888-7111

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

Fax: +1-519-888-0677

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

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

#### **© 2025 Open Text**

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

#### **Disclaimer**

##### **No Warranties and Limitation of Liability**

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

---

# Table of Contents

<b>1</b>	<b>Overview .....</b>	<b>9</b>
1.1	Logging in to Documentum Administrator .....	9
1.2	System Information page .....	11
1.3	Determining the Documentum Administrator version .....	13
1.4	Preferences .....	13
<b>2</b>	<b>OpenText Documentum CM license activation .....</b>	<b>15</b>
<b>3</b>	<b>Basic configuration .....</b>	<b>17</b>
3.1	Adding a connection broker for one session .....	17
3.2	Tracking software usage .....	17
3.3	Managing repositories .....	17
3.4	Windows domain authentication for Linux repositories .....	53
3.5	Managing Documentum CM Servers .....	53
3.6	Federations .....	73
3.7	Java Method Servers .....	78
3.8	LDAP servers .....	87
3.9	LDAP Certificate Database Management .....	104
<b>4</b>	<b>Distributed configurations .....</b>	<b>107</b>
4.1	Network locations .....	107
4.2	Accelerated Content Services servers .....	112
4.3	Branch Office Caching Services servers .....	120
4.4	Configuring distributed transfer settings .....	126
4.5	Messaging server configuration .....	128
<b>5</b>	<b>System reports .....</b>	<b>131</b>
5.1	System overview report .....	131
5.2	User list report .....	133
5.3	User activity report .....	134
5.4	Transaction report .....	134
5.5	External transaction activity report .....	135
5.6	End user report .....	135
5.7	Occasional user role report .....	136
<b>6</b>	<b>User management .....</b>	<b>137</b>
6.1	Administering users, groups, roles, and sessions .....	137
6.2	Users .....	138
6.3	Groups .....	155
6.4	Roles .....	164
6.5	Module roles .....	167
6.6	Sessions .....	170

<b>7</b>	<b>Security .....</b>	<b>173</b>
7.1	Permission sets .....	173
<b>8</b>	<b>Audit management .....</b>	<b>185</b>
8.1	Auditing .....	185
8.2	Auditing by object type .....	185
8.3	Auditing by object instance .....	187
8.4	Auditing by events selected for all objects in the repository .....	189
8.5	Search audit .....	190
8.6	Audit policies .....	192
8.7	Registering audits .....	194
8.8	Adding, modifying, or removing audits .....	195
8.9	Verifying or purging audit trails .....	195
<b>9</b>	<b>Job management .....</b>	<b>197</b>
9.1	Jobs .....	197
9.2	Methods .....	243
9.3	Administration methods .....	252
<b>10</b>	<b>Alias sets and aliases .....</b>	<b>289</b>
10.1	Alias sets and aliases .....	289
10.2	Creating or modifying alias sets .....	289
10.3	Viewing or removing aliases .....	290
10.4	Adding or modifying aliases .....	291
10.5	Deleting alias sets .....	292
<b>11</b>	<b>Formats .....</b>	<b>293</b>
11.1	Overview .....	293
11.2	Viewing, creating, or modifying formats .....	293
11.3	Deleting formats .....	295
<b>12</b>	<b>Types .....</b>	<b>297</b>
12.1	Managing types .....	297
12.2	Creating or modifying types .....	298
12.3	Selecting a type .....	302
12.4	Deleting types .....	302
12.5	Viewing assignment policies .....	303
12.6	Converting types to shareable object types .....	304
12.7	Converting types to lightweight object types .....	304
12.8	Converting types to shareable and lightweight object types .....	305
<b>13</b>	<b>Storage management .....</b>	<b>307</b>
13.1	Storage management areas .....	307
13.2	Storage .....	307

13.3	Assignment policies .....	345
13.4	Migration policies .....	351
<b>14</b>	<b>Content delivery .....</b>	<b>357</b>
14.1	Content delivery services .....	357
14.2	Locating content delivery configurations .....	357
14.3	Creating or modifying content delivery configurations .....	359
14.4	Configuring the advanced properties of a content delivery configuration .....	361
14.5	Configuring replication properties for a content delivery configuration	366
14.6	Configuring extra arguments for a content delivery configuration .....	367
14.7	Deleting content delivery configurations .....	379
14.8	Testing content delivery configurations .....	380
14.9	Duplicating a content delivery configuration .....	381
14.10	Deactivating a content delivery configuration .....	381
14.11	Publishing objects .....	382
14.12	Content delivery configuration results .....	384
14.13	Content delivery logs .....	384
14.14	Effective labels .....	385
<b>15</b>	<b>Indexing management .....</b>	<b>387</b>
15.1	Indexing .....	387
15.2	Index agents and xPlore .....	387
15.3	Starting and stopping index agents .....	387
15.4	Disabling index agents .....	388
15.5	Enabling index agents .....	389
15.6	Verifying indexing actions .....	389
15.7	Viewing or modifying index agent properties .....	389
15.8	Managing index queue items .....	390
<b>16</b>	<b>Transformation Services management .....</b>	<b>393</b>
16.1	Transformation Services .....	393
16.2	Changing the Transformation Services user .....	393
16.3	Configuring a Transformation Services instance .....	394
16.4	Viewing a Transformation Services log file .....	397
16.5	Viewing details of a Transformation Services instance .....	398
16.6	Controlling your Transformation Services instance .....	399
16.7	Transformation Services reporting .....	400
16.8	Viewing transformation request in queue .....	402
16.9	Transformation Services profiles .....	402
<b>17</b>	<b>Content Intelligence Services .....</b>	<b>407</b>
17.1	Overview .....	407

17.2	Configuring Content Intelligence Services in Documentum Administrator .....	409
17.3	Building taxonomies for classic categorization .....	413
17.4	Selecting and submitting the documents to analyze .....	435
17.5	Managing analysis results using Documentum Administrator .....	441
<b>18</b>	<b>Resource management .....</b>	<b>447</b>
18.1	Understanding Resource Management .....	447
18.2	Managing resource agents .....	447
18.3	Managing resource properties .....	450
<b>19</b>	<b>Administrator access .....</b>	<b>459</b>
19.1	Administrator access sets .....	459
<b>20</b>	<b>Client rights management .....</b>	<b>465</b>
20.1	Client rights domains and privileged clients .....	465
20.2	Client rights domains .....	465
20.3	Privileged clients .....	469
<b>21</b>	<b>Data visualization .....</b>	<b>475</b>
21.1	Configuring reporting servers .....	475
21.2	Viewing and running reports .....	476
21.3	OOTB reports .....	476
<b>22</b>	<b>Workflow calendars .....</b>	<b>497</b>
22.1	Creating a calendar .....	497
22.2	Editing a calendar .....	499
22.3	Deleting a calendar .....	499
<b>23</b>	<b>Administering business processes .....</b>	<b>501</b>
23.1	Introduction to process management .....	501
23.2	Finding process templates .....	502
23.3	Administering process instances .....	505
23.4	Administering tasks .....	507
23.5	Managing task details .....	510
<b>24</b>	<b>Cabinets, files, and virtual documents .....</b>	<b>513</b>
24.1	Creating cabinets .....	513
24.2	Creating folders .....	515
24.3	Creating files .....	515
24.4	Creating a form .....	516
24.5	Working with files .....	517
24.6	Deleting cabinets, folders, or files .....	527
24.7	Managing subscriptions .....	527
24.8	Enabling change notifications .....	528

24.9	Managing relationships .....	528
24.10	Renditions and transformations .....	529
24.11	Configuring PDF Annotation Service .....	531
24.12	Virtual documents .....	531
24.13	Email messages .....	536
<b>25</b>	<b>Inbox .....</b>	<b>537</b>
25.1	Inboxes .....	537
25.2	Opening a task or notification .....	537
25.3	Performing a task .....	537
25.4	Completing a task .....	538
25.5	Accepting a group task .....	539
25.6	Rejecting a task .....	539
25.7	Delegating a task .....	539
25.8	Repeating a task .....	540
25.9	Changing availability for tasks .....	540
25.10	Work queue tasks .....	541
<b>26</b>	<b>Search .....</b>	<b>543</b>
26.1	Searches .....	543
26.2	Setting search preferences .....	543
26.3	Search guidelines .....	544
26.4	Running a simple search .....	544
26.5	Running an advanced search .....	549
26.6	Viewing search results .....	554
26.7	Running an advanced search for archiving document in InfoArchive ..	556
26.8	Viewing search results and archiving document in InfoArchive .....	561
26.9	Additional configuration options .....	562
26.10	Saved searches .....	563
26.11	Creating a search template .....	564
<b>27</b>	<b>Tools .....</b>	<b>567</b>
27.1	The Tools menu .....	567
27.2	Lifecycles .....	567
27.3	Workflows .....	569
27.4	Work queue management .....	575
27.5	DQL editor .....	596
27.6	API tester .....	596
27.7	Install DAR .....	597
<b>28</b>	<b>Content Services for SAP Web Administrator .....</b>	<b>599</b>
28.1	SAP Web Administrator .....	599
28.2	Configuring Connections to SAP .....	600

28.3	Configuring HTTP Archiving Services .....	602
28.4	Agent component .....	605
28.5	Configuring the Manage and View Components .....	612
<b>29</b>	<b>My Documentum for Microsoft Outlook administration ....</b>	<b>615</b>
29.1	My Documentum for Microsoft Outlook .....	615
29.2	Overview page .....	616
29.3	Profiles .....	616
29.4	Client Setup .....	620

# Chapter 1

## Overview

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

Documentum Administrator is a web-based administration tool for most of the OpenText™ Documentum™ Content Management Server administration tasks.

The users of Documentum Administrator are OpenText Documentum Content Management (CM) administrators, Content Intelligence Services administrators and taxonomy managers, and OpenText™ Documentum™ Content Management Transformation Services 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

[“Logging in to Documentum Administrator” on page 9](#) provides URL and login information.

*OpenText Documentum Content Management - Server and Server Extensions Installation Guide (EDCSY250400-IGD)* provides information about installing Documentum Administrator.

### 1.1 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. OpenText recommends 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, type the following information:

Field	Description
<b>Login Name</b>	Your login name.
<b>Password</b>	Your login password.
<b>Repository</b>	Select a repository from the list. If you change the repository, retype your password.
<b>Locations</b>	In the <b>Location</b> 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.
<b>Remember my credentials</b>	Select to have the system remember your credentials, so you do not have to type them again the next time you log in.
<b>More options</b>	
<b>Domain</b>	If the repository is running in domain-required mode, type the domain name.
<b>Language</b>	To set the session locale to another language, select the language from the drop-down list.
<b>Server</b>	To connect to the repository using a particular server, select that server from the <b>Server</b> list box. The default is <b>Any Running Server</b> .
<b>Additional Accessibility Options</b>	Select <b>Additional Accessibility Options</b> on the login page to enable the accessibility options.

Field	Description
<b>Change Password</b>	To change your password in a repository, click <b>Change Password</b> , select a repository, and type your old and new passwords, then click <b>Change Password</b> . 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.

4. Click **Login**.

The **System Information** page appears with information about the system. For more information, see “[System Information page](#)” on page 11.



### Caution

To log in to Documentum Administrator and connect to a repository which is using a OpenText Documentum Content Management (CM) Server in dormant state, the user needs to be a member of the dm\_datacenter\_managers privileged group.

## 1.2 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.

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

**Table 1-1: System Information page**

Field	Description
<b>User</b>	The user name under which you are connected.
<b>Repository</b>	
<b>Repository</b>	The repository to which you are connected.
<b>Federation</b>	The federation to which the current repository belongs, if any.
<b>Global Repository</b>	The name of the global repository.

Field	Description
<b>Dormancy Status</b>	Indicates the dormancy status of repository.   <b>Note:</b> The Dormancy Status label is only visible for 7.0 and later versions of repositories.
<b>Content Storage Service</b>	Indicates if Content Storage Services is available.
<b>Content Intelligence</b>	Indicates whether Content Intelligence Services is enabled. If Content Intelligence Service is enabled, click <b>Configure</b> to access the <b>Configuration for Content Intelligence</b> page.
<b>Documentum Server</b>	
<b>Documentum Server</b>	The Documentum CM Server to which you are connected.
<b>Server Version</b>	The Documentum CM Server version and platform.
<b>Trusted Mode</b>	Indicates if OpenText™ Documentum™ Content Management Trusted Content Services is available in the repository to which you are connected.
<b>Dormancy Status</b>	Indicates the dormancy status of Documentum CM Server.   <b>Note:</b> The Dormancy Status label is only visible for 7.0 and later versions of Documentum CM Server.
<b>Hostname</b>	The host name of the Documentum CM Server to which you are connected.
<b>Distributed Content</b>	
<b>Network Locations</b>	The number of network locations associated with the repository.
<b>BOCS Servers</b>	The number of OpenText™ Documentum™ Content Management Branch Office Caching Services servers associated with the repository.
<b>ACS Read</b>	Indicates if users can read content in the repository through the OpenText™ Documentum™ Content Management Accelerated Content Services.

Field	Description
<b>ACS Dormancy Status</b>	Indicates the dormancy status of OpenText Documentum Content Management (CM) Accelerated Content Services server.   <b>Note:</b> The Dormancy Status label is only visible for 7.0 and later versions of Accelerated Content Services server.
<b>Messaging</b>	Indicates whether the messaging server is enabled.
<b>ACS Server</b>	The name of the Accelerated Content Services server.
<b>ACS Write</b>	Indicates if users can write content to the repository through the Accelerated Content Services and whether the write is synchronous or asynchronous.
<b>BOCS Pre-caching</b>	Indicates if the repository is enabled to process pre-caching requests.
<b>LDAP Servers</b>	
<b>Enabled Servers</b>	The number of enabled LDAP servers.
<b>Disabled Servers</b>	The number of disabled LDAP server.
<b>Last Sync</b>	The time and date the Documentum CM Server and LDAP servers were last synchronized.

## 1.3 Determining the Documentum Administrator version

From the **System Information** page, select **File > About Administrator** to determine the Documentum Administrator version.

## 1.4 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.



## Chapter 2

# OpenText Documentum CM license activation

OpenText Documentum CM uses OpenText Directory Services (OTDS) to apply licenses for all the OpenText Documentum CM components. For more information about procuring the license file and configuring OTDS and license, see *OpenText Documentum Content Management - Server and Server Extensions Installation Guide (EDCSY250400-IGD)*.

### To activate the license:

1. Connect to Documentum Administrator as an installation owner using the following URL format:

```
https://<Ingress Controller URL>/da?skipssso=true
```

For example:

```
https://otgcp.documentum.net/da?skipssso=true
```

2. Go to **Administration > Basic Configuration > Repository** to access the **Repository** list page.
3. Select the repository name and select **View > Properties > Info**.
4. Click the **OTDS License Configuration** tab.
5. Provide the appropriate information as described in the following table:

Field	Description
<b>OTDS URL</b>	The OTDS REST web address using the HTTP or HTTPS protocol. The web address format for the following environments is as follows: <ul style="list-style-type: none"><li>• On-premises: <code>http(s)://&lt;IP address of the OTDS machine&gt;:&lt;port&gt;/otdswebs/rest</code></li><li>• Cloud: <code>http(s)://&lt;host name of the OTDS machine&gt;.&lt;OpenText Documentum CM Ingress web address&gt;/otdswebs/rest</code></li></ul> Or <code>http://otdswebs:&lt;port&gt;/otdswebs/rest</code>
<b>Business Admin Username</b>	The name of the OTDS user in the <code>otds.admin</code> partition.
<b>Business Admin Password</b>	The password for the OTDS user.

Field	Description
<b>Confirm Password</b>	Retype the password for the OTDS user for verification.
<b>Validate and Fetch License Key: Validate</b>	Click <b>Validate</b> to validate and fetch the OpenText Documentum CM license key(s) added in OTDS.
<b>License key</b>	The list of OpenText Documentum CM license key(s) added in OTDS. Select the required license key from the list.

6. Click **OK** to activate the license key.



**Note:** You can click **Edit** for modifications, if required. You can modify the licensing information either as an installation owner or superuser (with the appropriate application role in OTDS).

## Chapter 3

# Basic configuration

### 3.1 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 following format:

```
connection_broker_name:port_number
```

For example: mozart:1756

### 3.2 Tracking software usage

Documentum CM Server only provides basic report for the system administrator. “[Usage tracking \(dm\\_usageReport\)](#)” on page 210 provides more information.

### 3.3 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 Documentum CM Server installer.

**Table 3-1: Information on the repository page**

Field	Description
<b>Name</b>	The name of the repository configuration object of the repository.
<b>DBMS</b>	The underlying database used for the repository.
<b>Federation</b>	The federation to which the repository belongs.
<b>Effective Date</b>	The effective date of the docbase configuration object. The effective date is used to manage client query caches.
<b>Dormancy Status</b>	<p>The current dormancy status of the repository. Valid values are:</p> <ul style="list-style-type: none"> <li>• <b>Dormancy Requested</b></li> <li>• <b>Dormant</b></li> <li>• <b>Active</b></li> <li>• <b>Invalid</b></li> </ul> <p> <b>Note:</b> The Dormancy Status column is only visible for 7.0 and later versions of repositories.</p>

### 3.3.1 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**.
4. On the **Repository Configuration Properties - Info** page, modify the values that you want to change, as described in “[Repository configuration properties](#)” on page 19.
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 OpenText Documentum CM Offline Client.  
“[Modifying repository synchronization](#)” on page 24 provides more information.

7. Click **OK** to accept the changes or **Cancel** to discard the modifications.

**Table 3-2: Repository configuration properties**

Field	Description
<b>Database</b>	The name of the RDBMS vendor. Read-only.
<b>Repository ID</b>	The repository ID number assigned during installation. Read-only.
<b>Federation</b>	Specifies if the repository is a member of a federation. Read-only.
<b>Security</b>	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.
<b>Index Store</b>	The name of the tablespace or other storage area where type indexes for the repository are stored.
<b>Partitioned</b>	Indicates whether the repository is partitioned. When a repository is created or updated with partitioning enabled, the Documentum CM Server sets the flag to True.  The Partitioned field is: <ul style="list-style-type: none"> <li>• Not selectable or changeable.</li> <li>• Available only in 6.5 repositories and later.</li> </ul>
<b>Crypto Mode</b>	Displays the type of cryptography used by Documentum CM Server.
<b>Crypto Key Store</b>	Indicates the encryption key stored on the Documentum CM Server.
<b>Dormancy Status</b>	Indicates the dormancy status of repository.   <b>Note:</b> The Dormancy Status label is only visible for 7.0 and later versions of repositories.
<b>Update Configuration Changes</b>	
<b>Re-Initialize Server</b>	Select to reinitialize the server to which you are connected. This is necessary for changes to objects to take effect.
<b>Configuration Changes</b>	
<b>Folder Security</b>	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.
<b>Rich Media</b>	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.

Field	Description
<b>Workflow Packages</b>	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.
<b>Data Dictionary Locales</b>	Specifies the locale of the data dictionary. The default local is en (English). Click <b>Edit</b> to configure a different locale. The server must be reinitialized for any changes to be visible.
<b>Oldest Client Version</b>	Specifies which OpenText™ Documentum™ Content Management Foundation Java API version is used for chunked XML documents. The value must be changed manually. If the field is left blank, the OpenText Documentum Content Management (CM) Foundation Java API format is compatible with previous versions of clients also. If a particular Foundation Java API version is specified, clients running an earlier Foundation Java API 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.
<b>Modifications Comment</b>	This field is optional. It can be used to add a comment about any modifications made to the repository configuration.
<b>Default Application Permit</b>	<p>The default user permission level for application-controlled objects accessed through an application that does not own the object. Valid values are:</p> <ul style="list-style-type: none"> <li>• 2: Browse</li> <li>• 3: Read</li> <li>• 4: Relate</li> <li>• 5: Version</li> <li>• 6: Write</li> <li>• 7: Delete</li> </ul> <p>The default value is 3, Read permission.</p>
<b>Fulltext Install Locations</b>	Specifies the Verity versions installed and their locations in pre-5.3 repositories.
<b>Content Storage Services Enabled</b>	Specifies if Content Storage Services is available.

Field	Description
<b>Minimum Owner Permission</b>	<p>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:</p> <ul style="list-style-type: none"> <li>• Browse</li> <li>• Read</li> <li>• Relate</li> <li>• Version</li> <li>• Write</li> <li>• Delete</li> </ul> <p>The default value is <b>Browse</b>.</p>
<b>Minimum Owner Extended Permission</b>	<p>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:</p> <ul style="list-style-type: none"> <li>• Execute Procedure Users with superuser privileges can change the owner of an item and run external procedures on certain types.</li> <li>• Change Location Allows the object owner to move the object in the repository.</li> <li>• Change State Allows the object owner to change the state of a lifecycle attached to the object.</li> <li>• Change Permission Allows the object owner to modify the basic permissions associated with the object.</li> <li>• Change Ownership Allows the object owner to change the object owner.</li> <li>• Extended Delete Allows the object owner to delete the object.</li> <li>• Change Folder Links Allows the folder owner to link or unlink other objects to this folder.</li> </ul>
<b>Authorization Settings</b>	

Field	Description
<b>MAC Access Protocol</b>	<p>The file-sharing software type in use for Macintosh clients. Valid values are:</p> <ul style="list-style-type: none"> <li>• None</li> <li>• NT</li> <li>• Ushare</li> <li>• Double</li> </ul> <p>The default value is None.</p> <p>If you change the value from NT, Ushare, or Double to None, existing resource forks are no longer be accessible.</p> <p>To change the value from or to NT, Ushare, or Double, you must first change the value to None, save the configuration, and then change it from None to the new value.</p>
<b>Authentication Protocol</b>	<p>Defines the authentication protocol used by the repository.</p> <ul style="list-style-type: none"> <li>• On Windows, if set to Domain Required, it indicates that the repository is running in domain-required mode.</li> </ul> <p>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 their login domain name when logging into the repository.</p> <p>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.</p> <ul style="list-style-type: none"> <li>• On Linux platforms, choose between Linux authentication or Windows domain authentication.</li> </ul>
<b>Cached Query Effective Date</b>	<p>Used to manage the client query caches. The default is NULLDATE.</p>
<b>Run Actions As</b>	<p>The user account that is used to run business policy (document lifecycle) actions. Options are:</p> <ul style="list-style-type: none"> <li>• Session User (default)</li> <li>• Superuser</li> <li>• Lifecycle Owner</li> <li>• Named User</li> </ul> <p>If selected, click the <b>Select User</b> link to access the Choose a user page to select a user.</p>

Field	Description
<b>Login Tickets</b>	<p>Specifies that all other repositories are trusted and login tickets from all repositories are accepted by the current repository.</p> <p>If selected, <b>Allow login tickets from repositories</b> is not displayed.</p>
<b>Allow login tickets from repositories</b>	<p>This field is only displayed if <b>Allow all login tickets</b> is not selected.</p> <p>Click <b>Select</b> to access the Choose Repositories page to designate repositories whose login tickets are permitted in the current repository (the trusted repositories).</p>
<b>Designate Login Ticket Expiration</b>	<p>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:</p> <ul style="list-style-type: none"> <li>• <b>Null date:</b> Specifies that there is no cutoff date for login tickets in the current repository. This is the default value.</li> <li>• <b>Expire login tickets on the following date and time:</b> Specifies the earliest possible creation date for valid login tickets. Use the calendar control to choose the correct date and time.</li> </ul> <p>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.</p>
<b>Maximum Authentication Attempts</b>	<p>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.</p> <p>By default, the account of installation owner 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.</p> <p>A value of zero (0) means that the feature is not enabled.</p> <p>Requires the server to be reinitialized for changes to take effect.</p>
<b>LDAP Synchronization On-Demand</b>	<p>Used to synchronize LDAP directory users with the repository between scheduled runs of the LDAP synchronization job:</p> <ul style="list-style-type: none"> <li>• When cleared, LDAP directory users who do not exist in the repository cannot log in.</li> <li>• When selected, if an LDAP directory user attempts to log in and is found not to exist in the repository, Documentum CM 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.</li> </ul>

Field	Description
<b>Privileged Clients</b>	Boolean. If selected, indicates that the repository is accessible to privileged clients only.  This check box is only available if a Foundation Java API client exists in the repository and is approved to perform privilege escalations.

### 3.3.2 Modifying repository synchronization

The synchronization options control the behavior of OpenText Documentum CM 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 OpenText Documentum CM 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**.
4. Click the **Synchronization** tab.
5. Modify the values, as described in “[Synchronization properties](#)” on page 25.
6. Click **OK** to accept the changes.

**Table 3-3: Synchronization properties**

Field	Description
<b>Synchronization Settings</b>	<p>For repositories where Offline Client is enabled. Options are:</p> <ul style="list-style-type: none"> <li>• None: no content synchronization to local machine.</li> <li>    No content is synchronized to the local machine. This is the default setting for a repository.</li> <li>• Basic: 1-way download to local machine as read only.</li> <li>    Content is downloaded to the local machine and marked read-only. No content is uploaded from the local machine.</li> <li>• Role-Based: assign sync permissions to specific repository roles.</li> <li>    Synchronization permissions are based on specific user roles. Synchronization is enabled and users can download content. Whether content can be uploaded depends on the role of a particular user. If selected, you must designate the synchronization roles and check-in settings.</li> </ul>
<b>Synchronization Role</b>	<p>If you selected role-based synchronization where Offline Client is enabled, you must designate the roles. Click the <b>Select users/groups for offline upload</b> link to access the Choose a user/group page to select users who you want to use offline upload.</p>
<b>Check In Settings</b>	<p>Select to use the client dialog or the local settings of user to check content into the repository. Options are:</p> <ul style="list-style-type: none"> <li>• Always Use client dialog to check in content</li> <li>• Use User's local check in setting</li> </ul>

### 3.3.3 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**.
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.



#### Notes

- When a repository is moved to a dormant state, the status of all the Documentum CM Servers and Accelerated Content Services servers for this repository will also be moved to a dormant state.
- In a multiple Documentum CM Server setup, moving a repository to a dormant state will move all the configured Documentum CM 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**.

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.



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

### 3.3.4 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 Foundation Java API 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 Foundation Java API installation to contact the global registry.

#### To modify the `dfc.properties` file manually:

1. On the Foundation Java API host, navigate to `$DOCUMENTUM/config` (Linux) or `%DOCUMENTUM%\config` (Windows).
2. From a command prompt, run 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_namedfc.globalregistry.user
name=user_login_namedfc.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.

### 3.3.5 Repository content

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

[“Default users created during repository configuration” on page 28](#) lists the default users that are created during repository configuration.

**Table 3-4: Default users created during repository configuration**

User	User privileges	Extended user privileges
repository_owner	Superuser	None
installation_owner	Superuser	None
global registry user	None	None
dm_bpm_inbound_user	None	None
dm_autorender_win32	System Administrator	None
dm_autorender_mac	System Administrator	None
dm_mediaserver	System Administrator	None
dm_fulltext_index_user	Superuser	None

The configuration program creates a number of default groups. [“Default groups created during repository configuration” on page 28](#) describes the default groups. In addition to the default groups, the configuration program also creates a set of privileged groups. [“Privileged groups” on page 157](#) provides more information about privileged groups.

**Table 3-5: Default groups created during repository configuration**

Group	Members
admingroup	installation_owner, repository_owner

Group	Members
docu	repository_owner, installation_owner, dm_autorender_win32, dm_autorender_mac, dm_mediaserver
queue_admin	None
queue_manager	queue_admin group
queue_processor	queue_manager group
process_report_admin	queue_admin

### 3.3.6 Type indexes

Indexes on the object type tables in the RDBMS enhance the performance of repository queries. When a repository is configured, the Documentum CM 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" on page 277](#) 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" on page 278](#) provides more information about the MAKE\_INDEX method.

*OpenText Documentum Content Management - Server and Server Extensions Installation Guide (EDCSY250400-IGD)* 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" on page 271](#) provides more information about the DROP\_INDEX method.

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

### 3.3.7 Date values

By default, Documentum CM Server stores date values as UTC (Coordinated Universal Time) time in new repositories (OpenText Documentum CM 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 Documentum CM 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, Documentum CM Server stores all date values based on the time identified by the time zone offset.

In a OpenText Documentum CM 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 Documentum CM Server local time and cannot be changed.

### 3.3.8 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 as the source repository.

Dump and load operations can be performed manually using either IAPI, Docbasic scripts, or the `IDfDumpRecord` and `IDfLoadRecord` Foundation Java API interfaces.



**Note:** Dump and load operations require additional steps for repositories where Web Publisher is installed.

### 3.3.8.1 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 Documentum CM Server which objects to copy into the specified file.

- Dump Object Record (dmi\_dump\_object\_record)

A dump 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 Documentum CM 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.

*OpenText Documentum Content Management - Server System Object Reference Guide (EDCCS250400-ORD)* provides information about the properties of these object types.

### 3.3.8.2 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.

### 3.3.8.3 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.

### 3.3.8.4 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.

### 3.3.8.5 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. *OpenText Documentum Content Management - Server System Object Reference Guide (EDCCS250400-ORD)* contains more information.

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.

#### 3.3.8.5.1 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 Documentum CM 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 dmrContainment.

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 definition of subtype. 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*:

```
append,c,1,type
your_type_nameappend,c,1,predicate
1=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):

```
append,c,1,type
dm_acl
append,c,1,predicate
1=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, Documentum CM 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.

### 3.3.8.5.2 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. *OpenText Documentum Content Management - Server DQL Reference Guide (EDCCS250400-DRD)* 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, Documentum CM 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. Documentum CM 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.

### 3.3.8.6 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, 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. Documentum CM Server decrypts the content before placing it into the dump file.

[“Dumping without content” on page 35](#) describes the default behavior and requirements for handling dump files without content. [“Including content” on page 36](#) 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.

#### 3.3.8.6.1 Dumping without content

By default, a dump operation on content in file stores, 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 address of the content.

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 account to read the files in the source repository and copy them into the target repository.

### 3.3.8.6.2 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 Documentum CM Server dumps an object with content, the content is copied into the dump file also. The content must be stored in a file store, Centera store, or NetApp SnapLock storage area. Documentum CM 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.

### 3.3.8.6.3 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`.

Documentum CM Server automatically decompresses a compressed dump file during a load operation.

### 3.3.8.7 Setting the cache size

Documentum CM Server uses an in-memory cache to store the object IDs of dumped objects. Before dumping an object, Documentum CM 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.

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

### 3.3.8.8 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.

### 3.3.8.9 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, Documentum CM 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.

### 3.3.8.9.1 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 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 1=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
dumpfile name# Supply your own file name.
# This must be a new file
append,c,1,type
dm_sysobject
append,c,1,predicate
1=1
append,c,1,type
dm_assembly
append,c,1,predicate
1=1
append,c,1,type
dm_format
append,c,1,predicate
1=1
append,c,1,type
dm_user
append,c,1,predicate
1=1
append,c,1,type
dm_group
append,c,1,predicate
1=1
append,c,1,type
dmi_queue_item
append,c,1,predicate
1=1
append,c,1,type
dmi_registry
append,c,1,predicate
1=1
append,c,1,type
dm_relation
append,c,1,predicate
```

```

1=1
append,c,1,type
dm_relation_type
append,c,1,predicate
1=1
append,c,1,type
dmr_containment
append,c,1,predicate
1=1
append,c,1,type
dmr_content
append,c,1,predicate
1=1
append,c,1,dump_parameter
cache_size=60 #set cache size
append,c,1,dump_parameter
restartable=F #non-restartable dump
append,c,1,predicate
1=1
save,c,1
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, Documentum CM 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,1,type
your_type_nameappend,c,1,predicate
1=1

```

#### 3.3.8.10 If the server crashes during a dump operation

If Documentum CM 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. Documentum CM Server begins where it left off when the crash occurred.

### 3.3.8.11 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.

### 3.3.8.12 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 index. You can turn off this behavior.

[“Turning off save event generation during load operations” on page 41](#) 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 Documentum CM 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.

### 3.3.8.12.1 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.

### 3.3.8.12.2 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.

### 3.3.8.12.3 Loading registered tables

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

### 3.3.8.12.4 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:

```
generate_event=F
```

### 3.3.8.12.5 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 cabinet of the repository owner was modified, use the following command sequence to obtain a listing of its property values:

```
fetch,c,cabinet_iddump,c,1
```

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.

### 3.3.8.12.5.1 The preLoad utility

You can use the preLoad utility that runs 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.

### 3.3.8.12.6 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. Documentum CM 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 owner of the new repository 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 fulltext 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” on page 43.
4. Create and save the following script:

```
create,c,dm_load_record
set,c,1,file_name
full_path_of_dump_filesave,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:

```
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. Documentum CM Server does not overwrite an existing dump file with another dump file of the same name.
- If Documentum CM Server crashes during a load, you can fetch the Load Object and save it again, to restart the process. Documentum CM Server begins where it left off when the crash occurred.

#### 3.3.8.12.7 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.

#### 3.3.8.13 Generating dump and load trace messages

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

To activate tracing, use a setServerTraceLevel method.

The trace information includes:

- Whether Documentum CM 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

### 3.3.9 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 IDfSysObject.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 Javadocs 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 \(dm\\_DMclean\)” on page 202](#) 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.

Documentum CM 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.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.

### 3.3.10 Checking consistency

Documentum CM 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 OpenText Global Technical Services 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](#)” on page 240 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.

OpenText recommends that you run this tool on a repository before upgrading the repository to a new version of the Documentum CM Server.

#### 3.3.10.1 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.

#### 3.3.10.2 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
## ##     but missing r_accessor_permit 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

#####
## ## CONSISTENCY_CHECK: Sysobjects
## ## ##      Start Time: 09-10-2002 10:15:58
## ## ## #####
## ## 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
#####
## 
## 
## CONSISTENCY_CHECK: Folders and Cabinets
##
##      Start Time: 09-10-2002 10:16:02
##
#####
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
#####
## 
## 
## CONSISTENCY_CHECK: Documents
##
## 
## 
##      Start Time: 09-10-2002 10:16:03
##
#####
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-existen  
t 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  
  
#####  
##  
##  
## 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 propertys that are
no longer in dm_type
#####
###
###
## ## CONSISTENCY_CHECK: Indices
###
##      Start Time: 09-10-2002 10:16:11
###
#####

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
#####
###
###
## ## CONSISTENCY_CHECK: Methods
###
##      Start Time: 09-10-2002 10:16:11
###
#####

Checking for java dm_method objects that reference
jview

```

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

### 3.3.11 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:  

```
dm_encrypt_password -docbase <docbase_name> -rdbms -encrypt <database_password>
```
5. Start the repository.

### 3.3.12 Tracing options

A variety of tracing operations can be initiated on the Documentum CM Server through Documentum Administrator.

**To start or stop tracing on the repository:**

1. Navigate to **Administration > Basic Configuration > Repository**.
2. Select a repository on which tracing needs to be started or stopped and perform one of the following:
  - Select **Tools > View Tracing Options**.
  - Right-click on the repository and from the context-menu, choose **View Tracing Options**.

In the **Tracing options** page, you can find a drop-down list with a variety of options along with a brief description of the tracing.

3. Select the type of tracing from the drop-down list and click **Enable** or **Disable**.

## 3.4 Windows domain authentication for Linux repositories

Windows domain authentication for Linux repositories is not supported in Documentum Administrator.

## 3.5 Managing Documentum CM Servers

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

Each Documentum CM Server is associated with a server configuration object. A server configuration object is a template for a Documentum CM 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 Documentum CM Server configuration page in Documentum Administrator, as described in “[Server configuration object information](#)” on page 53.

Server configuration objects are stored in the repository System cabinet. You can add Documentum CM 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.

*OpenText Documentum Content Management - Server and Server Extensions Installation Guide (EDCSY250400-IGD)* provides information about creating, starting, and stopping a Documentum CM Server that is remote.

**Table 3-6: Server configuration object information**

Field	Description
Name	The name of the server configuration object.
Host	The name of the host on which the Documentum CM Server associated with the server configuration object is running.

Field	Description
<b>Operational Status</b>	<p>The current running status and dormancy status separated by a comma of the Documentum CM Server. Valid values are:</p> <p>Running Status:</p> <ul style="list-style-type: none"> <li>• <b>Running</b></li> <li>• <b>Unknown</b></li> </ul> <p>Dormancy Status:</p> <ul style="list-style-type: none"> <li>• <b>Dormancy Requested</b></li> <li>• <b>Dormant</b></li> <li>• <b>Active</b></li> <li>• <b>Invalid</b></li> </ul> <p> <b>Note:</b> The Operational Status column will display only the current running status for Documentum CM Server versions prior to 7.0.</p>
<b>Version</b>	The version of the server configuration object.

### 3.5.1 Adding or modifying Documentum CM Servers

The **Documentum Server Configuration** page lists the server configuration objects of all Documentum CM Servers for the current repository. Each Documentum CM 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 > Documentum Servers**.
3. On the **Documentum Server Configuration** page, do one of the following:
  - To add a Documentum CM Server, select **File > New > Server Config**.
  - To modify the server configuration object of an existing Documentum CM Server, select the server configuration object in the Name column, then select **View > Properties > Info**.

**Table 3-7: Server Configuration properties tabs**

<b>Tab</b>	<b>Description</b>
<b>Info</b>	Select the <b>Info</b> 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. <a href="#">“Modifying general server configuration information” on page 56</a> provides the instructions.
<b>Connection Brokers</b>	Select the <b>Connection Brokers</b> tab to view or modify connection broker projections, as described in <a href="#">“Creating or modifying connection broker projections” on page 61</a> .
<b>Network Locations</b>	Select the <b>Network Locations</b> tab to view or modify the proximity values for the associated network locations, as described in <a href="#">“Creating or modifying network locations” on page 62</a> .
<b>App Servers</b>	Select the <b>App Servers</b> tab to add an application server for Java method execution, as described in <a href="#">“Creating or modifying application servers” on page 63</a> .
<b>Cached Types</b>	Select the <b>Cached Types</b> tab to specify which user-defined types are to be cached at server startup, as described in <a href="#">“Creating or modifying cached types” on page 64</a> .
<b>Locations</b>	Select the <b>Locations</b> 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. <a href="#">“Creating or modifying locations” on page 65</a> provides instructions on creating or modifying locations.
<b>Far Stores</b>	Select the <b>Far Stores</b> tab to view accessible storage areas and to designate far stores, as described in <a href="#">“Creating or modifying far stores” on page 66</a> . A server cannot store content in a far store. <i>OpenText Documentum Content Management - Server and Server Extensions Installation Guide (EDCSY250400-IGD)</i> provides more information about far stores.

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” on page 56](#).

### 3.5.2 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 > Documentum Servers**.
2. On the **Documentum Server Configuration** page, select the server name to copy and then select **File > Save As**.
3. On the **Server Configuration Properties - Info** page, in the **Name** field, type the name of the new server configuration object.
4. Modify any properties that you want to change.  
*"Adding or modifying Documentum CM Servers" on page 54* provides information on modifying the other properties.
5. Click **OK** to save the new server configuration object or **Cancel** to exit.



**Note:** This option will be disabled if the Documentum CM Server is in dormant state for 7.0 and later versions of Documentum CM Server.

### 3.5.3 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 > Documentum Servers**.
2. On the **Documentum 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**.
3. Enter or modify the server configuration object properties, as described in the following table:

**Table 3-8: General server configuration properties**

Field	Description
<b>Name</b>	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.
<b>Host Name</b>	The name of the host on which the server is installed. Read-only.
<b>Server Version</b>	The version, operating system, and database of the server defined by the server configuration object. Read-only.
<b>Process ID</b>	The process ID of server on its host. Read-only.
<b>Install Owner</b>	The OpenText Documentum CM installation owner. Read-only.
<b>Install Domain</b>	On Windows, the domain in which the server is installed and running. Read-only.
<b>Trusted Mode</b>	Indicates if OpenText Documentum Content Management (CM) Trusted Content Services is available. Read-only.
<b>Dormancy Status</b>	Indicates the dormancy status of Documentum CM Server.  Note: The Dormancy Status label is only visible for 7.0 and later versions of Documentum CM Server.
<b>Update Configuration Changes</b>	
<b>Re-Initialize Server</b>	Select to reinitialize the server after the server configuration object is saved.
<b>Configuration Changes</b>	
<b>Web Server Location</b>	The name of the web server host and its domain. Used by client applications for creating DRLs.
<b>Web Server Port</b>	Identifies the port the web server uses. The default is 80.
<b>Agent Launcher</b>	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 Documentum CM 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 <b>Select Agent Launcher Method</b> link to access the Choose a method page.

Field	Description
<b>Operator Name</b>	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 <b>Select Operator</b> link to access the Choose a user page.
<b>Server Cache Size</b>	The maximum number of objects allowed in the server cache. The default is 200.
<b>Client Cache Size</b>	The maximum permitted size of the client cache, expressed as the number of objects. The default is 50.
<b>Network File Share</b>	Indicates whether the server is using Network File Share for file sharing.
<b>Checkpoint Interval</b>	Defines the interval at which the server broadcasts service information to connection brokers. The unit of measurement is seconds. The default is 300 seconds.
<b>Keep Entry Interval</b>	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 broadcast information of server.  By default, the value is 1,440 minutes (24 hours).
<b>Locale Name</b>	Indicates the server locale.  The value is determined during server installation.
<b>Default Client Codepage</b>	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.  Options are: <ul style="list-style-type: none"> <li>• UTF-8</li> <li>• ISO_8859-1</li> <li>• Shift_JIS</li> <li>• EUC-JP</li> <li>• EUC-KR</li> <li>• US-ASCII</li> <li>• ISO_10646-UCS-2</li> <li>• IBM850</li> </ul>

Field	Description
<b>Server OS Codepage</b>	<p>The code page used by the operating system of the machine on which the server resides. The value is determined programmatically and is set during server installation. In general, this value is not changed.</p> <p>Options are:</p> <ul style="list-style-type: none"> <li>• UTF-8</li> <li>• ISO_8859-1</li> <li>• Shift_JIS</li> <li>• EUC-JP</li> <li>• EUC-KR</li> <li>• US-ASCII</li> <li>• ISO_10646-UCS-2</li> <li>• IBM850</li> </ul>
<b>Turbo Backing Store</b>	<p>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.</p>
<b>Rendition Backing Store</b>	<p>The name of the file store storage area where the server will store renditions generated by full-text indexing operations.</p>
<b>Modifications Comments</b>	<p>Remarks on changes made to the server configuration object in this version.</p>
<b>SMTP Server</b>	<p>The name of the computer hosting the SMTP Server that provides mail services to Documentum CM Server.</p> <p>The value is provided during server installation.</p>
<b>Workflow Agent Worker Threads</b>	<p>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.</p>
<b>Secure Connect Mode</b>	<p>Specifies whether type of connection the server accepts.</p> <p>Options are:</p> <ul style="list-style-type: none"> <li>• Dual: Uses encrypted and unencrypted connections.</li> <li>• Native: Uses unencrypted connections only.</li> <li>• Secure: Uses encrypted connections only.</li> </ul> <p>If you change the mode, you must restart the server. Re-initializing the server does not suffice.</p>
<b>Maximum Content Migration Threads</b>	<p>Defines a valid value range for the argument PARALLEL_DEGREE for parallel content migration when running MIGRATE_CONTENT administration method or setting up a migration policy rule. Valid values are between 2 and 50.</p> <p>This option requires Content Storage Services on Documentum CM Server.</p>

Field	Description
<b>System Shutdown Timeout</b>	<p>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.</p> <p>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 Documentum CM Servers.</p> <p>If the timeout period is exceeded (or is set to zero), Documentum CM Server takes over and shuts down the workflow agent immediately.</p> <p>If the timeout period is a negative value, Documentum CM Server waits for the workflow agent threads to complete the automatic tasks held by workflow agent workers before shutting down gracefully.</p>
<b>Authorization Settings</b>	
<b>Inherit Permission Set From</b>	<p>The permission set the server uses for new objects if a user fails to specify a permission set for an object or fails to specify that no default permission set is wanted. Options are:</p> <p>A User permission set is defined for a user when a system administrator, superuser, or repository owner creates a user. This permission set can be used as the permission set for any object created by the user. Because user objects are not subtypes of SysObject, the permission set is not used to enforce any kind of security on the user. A User permission set can only be used as a default permission set.</p> <p>A Type permission set is associated with the type definition for a SysObject or SysObject subtype. A Type permission set can only be used as a default permission set.</p> <p>A Folder permission set is associated with a folder or cabinet. If a user wants to change a folder or properties of cabinet properties, modify the folder or cabinet object itself, or move, copy, or link an object to the folder, the server uses the permissions in the associated permission set to determine whether the user can perform the requested operation.</p>
<b>Default Alias Set</b>	The default alias set for new objects. Click the Select Alias Set link to access the Choose an alias set page.
<b>Enabled LDAP Servers</b>	<p>The LDAP configuration objects for LDAP servers used for user authentication and synchronization.</p> <p>Click the Select link to access the Choose LDAP Server Configurations page to add LDAP servers.</p>

Field	Description
<b>Maximum Login Ticket Expiration Time</b>	The maximum length of time, in minutes, that a login ticket generated by the current server can remain valid. The minimum value is 1 minute. The maximum value is 43200 minutes (30 days). The default value at server installation is 43200.
<b>Default Login Ticket Expiration Time</b>	The default length of time, in minutes, that a login ticket generated by the current server can remain valid. The value must always be less than or equal to the maximum login ticket expiration time. The default value is 5 minutes.
<b>Application Access</b>	Application access control (AAC) tokens are encoded strings that may accompany connection requests from applications. The information in a token defines constraints on the connection request. If selected, a connection request received by this server from a non-superuser must be accompanied by a valid application access control token and the connection request must comply with the constraints in the token.
<b>Superuser Access</b>	When selected, a user with superuser privileges cannot connect to the server using a global login ticket.

4. Do one of the following:

- If you are creating a server configuration object, click **Next** to configure connection brokers.
- If you are modifying an existing server configuration object, click **OK** to save your changes or click one of the other tabs to make additional changes.

### 3.5.4 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 Documentum CM Servers](#)” on page 54.

**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**.
2. Enter or modify the projection target information, as described in “[Projection target information](#)” on page 62.
  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 3-9: Projection target information**

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

### 3.5.5 Creating or modifying network locations

A network location identifies locations from which end users connect to OpenText Documentum CM web clients. Network locations define specific IP address ranges. Documentum CM 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 Documentum CM Servers](#)” on page 54.

**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 right arrow icon.
  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.

### 3.5.6 Creating or modifying application servers

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

Documentum CM 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 Documentum CM Servers](#)” on page 54.

#### 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, as described in “[Application server properties](#)” on page 64.
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.

**Table 3-10: Application server properties**

Field	Description
Name	Type the application server name.
URI	Type the URI to the application server, in the following format: <code>http://host_name:port_number/servlet_path</code>

### 3.5.7 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 Documentum CM Servers](#)” on page 54.

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

1. On the **Cached Types** page, you can:
  - Click **Add** to add one or more cached types.
  - 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 right arrow icon.
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.

### 3.5.8 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 Documentum CM Servers](#)” on page 54.

**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 “[Locations page properties](#)” on page 65.  
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 3-11: Locations page properties**

Field	Description
<b>Assume User</b>	The location of the directory containing the assume user program. The default is assume_user.
<b>Change Password</b>	The location of the directory containing the change password program. The default is change_password.
<b>Common</b>	The location of the common directory. The default is common.
<b>Events</b>	The location of the events directory. The default is events.
<b>Log</b>	The location of the logs directory. The default is temp.
<b>Nls</b>	The location of the NLS directory. The default is a single blank.
<b>Secure Writer</b>	The location of the directory containing the secure writer program. The default is secure_common_area_writer.

Field	Description
<b>System Converter</b>	The location of the directory containing the convert.tbl file and the system-supplied transformation scripts. There is no default for this field.
<b>Temp</b>	The location of the temp directory.
<b>User Converter</b>	The full path for the user-defined transformation scripts. The default is convert.
<b>User Validation</b>	The full path to the user validation program. The default is validate_user.
<b>Verity</b>	5.3 and later repositories, contains a dummy value for compatibility with Webtop 5.2.x. The default value is verity_location.
<b>Signature Check</b>	The location of the directory that contains the signature validation program. The default is validate_signature.
<b>Authentication Plugin</b>	The location of an authentication plug-in, if used. The default is auth_plugin in \$Documentum/dba/auth.

### 3.5.9 Creating or modifying far stores

In a Distributed Content environment, a far store is a storage area remote or inaccessible from the current Documentum CM Server, in which the server cannot store content. *OpenText Documentum Content Management - Server and Server Extensions Installation Guide (EDCSY250400-IGD)* 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 Documentum CM Servers](#)” on page 54.

**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 the right arrow icon.  
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.

### 3.5.10 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 Documentum CM 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 Documentum CM Server.

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

1. Navigate to **Administration > Basic Configuration > Documentum Servers**.
2. On the **Documentum 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**.
3. 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 system displays the **Documentum Server moved to dormant state successfully** message.



#### Notes

- You cannot copy a server configuration using **File > Save As** when the Documentum CM 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 Documentum CM 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 Documentum CM 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 Documentum CM Server.

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

1. Navigate to **Administration > Basic Configuration > Documentum Servers**.  
The **Documentum Server Configuration** list page appears.
2. Select a server configuration that needs to be made active.
3. On the **Documentum 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.



**Note:** You can also project the active or dormant state of Documentum CM Server to the connection broker. “[Projecting active or dormant state of Documentum CM Server to connection broker](#)” on page 69 contains the instructions.

### 3.5.11 Enabling or disabling save operation for a Documentum CM Server in dormant state

You can perform the enable or disable save operation for a Documentum CM 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 Documentum CM 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 Documentum CM Server.

**Caution**

To perform any of the view, create, update, or delete operations for a Documentum CM 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](#)” on page 67.

Use these instructions to perform the enable save operation:

**To perform enable save operation:**

1. Navigate to **Administration > Basic Configuration > Documentum Servers**.
2. Select the dormant server you want to enable save operation.
3. On the **Documentum 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**.

Use these instructions to perform the disable save operation:

**To perform disable save operation:**

1. Navigate to **Administration > Basic Configuration > Documentum Servers**.
2. Select the dormant server you want to disable save operation.
3. On the **Documentum 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**.

### 3.5.12 Projecting active or dormant state of Documentum CM Server to connection broker

The dormancy status of Documentum CM 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 Documentum CM Server.



#### Notes

- The **Project Dormant Status to Connection Broker** and **Project Active Status to Connection Broker** menu options are available only for Documentum CM Servers which is in active state. These options will not be available for Documentum CM 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](#)” on page 61.

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

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

1. Navigate to **Administration > Basic Configuration > Documentum Servers**.
2. Select the active server you want to project as dormant to the connection broker.
3. On the **Documentum 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**.

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

1. Navigate to **Administration > Basic Configuration > Documentum Servers**.
2. Select the active server you projected as dormant to project as active to connection broker.
3. On the **Documentum 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**.

### 3.5.13 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 > Documentum 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 \(dm\\_LogPurge\)](#)” on page 206 provides more information about the tool.

### 3.5.14 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 > Documentum Servers**.  
The **Server Configuration** list page appears.
2. Select the server configuration objects to delete.
3. Select **File > Delete**.  
The **Delete Object** page appears.
4. Click **OK** to delete the server configuration objects or **Cancel** to leave the server configuration objects in the repository.  
The Server Configuration list page appears.

#### 3.5.14.1 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.

### 3.5.15 Configuring a server as a process engine

If the Business Process Manager (BPM) application is installed in a repository and you have process engine, 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 > Documentum Servers**.
3. Select a server.
4. Select **Tools > Configure Process Engine**.
5. 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](#)” on page 72 provides more information.

### 3.5.16 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.

## 3.6 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 *OpenText Documentum Content Management - Server and Server Extensions Installation Guide (EDCSY250400-IGD)*.

### 3.6.1 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.

*OpenText Documentum Content Management - Server and Server Extensions Installation Guide (EDCSY250400-IGD)* 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 ["Federation properties" on page 74](#).

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

**Table 3-12: Federation properties**

Field	Description
<b>Info</b>	
<b>Name</b>	Type the name of the new federation.
<b>Make All Governing Repository Users &amp; Groups Global</b>	Select to make all users and groups in the governing repository global users and global groups.
<b>Active</b>	This option is available if you are modifying an existing federation. To change the status of an existing federation, select or clear the Active check box.
<b>User Subtypes</b>	
<b>Add</b>	Click <b>Add</b> to add user subtypes.  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 propagate to member repositories.

Field	Description
<b>Members</b>	
<b>Add</b>	<p>Click <b>Add</b> to add member repositories.</p> <p>Select the repositories that you want to be member repositories and click <b>Add</b>.</p> <p>Click <b>Edit</b> to edit a member repository. The <b>Edit</b> button will be available only after adding more than one repository.</p> <p>To remove any member repositories from the Selected Items list, select them and then click <b>Remove</b>.</p>
<b>Name</b>	The login name of a superuser account that is configured for the repository.
<b>Password</b>	The password of a superuser account this is configured for the repository.
<b>Skip this member and continue authentication</b>	Select this option if you want to skip entering the name and password at this time.

### 3.6.2 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 check box 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 check box next to any members that you want to remove and click **Remove**, then click **OK**.

7. Click **Finish**.

### 3.6.3 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** check box.

**To delete a federation:**

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

The federation is deleted.

### 3.6.4 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**.

### 3.6.5 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.

### 3.6.6 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**.

## 3.7 Java Method Servers

OpenText Documentum CM includes Java Method Server, a customized version of Tomcat to execute Documentum CM Server Java methods. One Java Method Server is installed with each Documentum CM 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 Documentum CM Server configuration program. *OpenText Documentum Content Management - Server and Server Extensions Installation Guide (EDCSY250400-IGD)* provides more information about installing multiple Documentum CM Servers, Java Method Servers, and the supported Java Method Server failover configurations.

OpenText Documentum CM provides a servlet called DO\_METHOD to execute Documentum CM Server methods. The compiled servlet code is found in the mthdservlet.jar file located on the same host as Documentum CM Server. The file contains the IDmMethod class. Java Method Server runs as an independent process. The process can be stopped or started without restarting the Documentum CM 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 Documentum CM 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. *OpenText Documentum Content Management - Server DQL Reference Guide (EDCCS250400-DRD)* provides details about the administration method.

Documentum Administrator provides a Java Method Server configuration page for:

- Viewing and updating Java Method Servers.
- Associating Documentum CM Servers with Java Method Servers.
- Viewing the Java Method Server status information in the Documentum CM Server memory cache.
- Resetting the Java Method Server information in the Documentum CM Server memory cache.

### 3.7.1 Viewing Java Method Server information

All available Java Method Servers 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 Java Method Server is represented by a Java Method Server configuration object. The Java Method Server Configuration page displays information for all Java Method Server configuration objects in the repository, as described in “[Java Method Server information](#)” on page 79.

**Table 3-13: Java Method Server information**

Field	Description
<b>Name</b>	The name of the Java Method Server configuration object.
<b>Is Enabled</b>	Specifies whether the Java method server is enabled or disabled.
<b>Associated Content Server</b>	The Documentum CM Server with which the Java Method Server configuration object is associated.

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 Server](#)” on page 83 provides more information.

If your Documentum CM Server version is 7.3 and later and if you have set the `JMS_HA_SETUP_ENABLED` attribute in `dm_docbase_config` object to `<true>`, Documentum Administrator provides the following option:

- Viewing and modifying the configuration of Java Method Server HA setup.
- Viewing and refreshing the status of all Java Method Server instances listed in the `dm_server_config` objects.

Then Java Method Server Configuration page lists the server configuration objects rather than the Java Method Server configuration objects.

### 3.7.2 Modifying Java Method Server configuration

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

**To modify Java Method Server configuration:**

1. Log in to the repository for which you want to modify the Java Method Server configuration.
2. Select **Administration > Basic Configuration > Java Method Servers**.
3. In the **Java Method Server Configuration** page, select the Java Method Server configuration you want to modify, then select **View > Properties > Info** or right-click the Java Method Server configuration object and select **Properties**.
4. In the **Java Method Server Configuration Properties** page, view or modify the information for the Java Method Server configuration, as described in “[Java Method Server configuration information](#)” on page 80.

**Table 3-14: Java Method Server configuration information**

Field	Description
<b>Name</b>	The name of the Java Method Server configuration.
<b>Enable</b>	Enables or disables the Java Method Server. Select this option to enable the Java Method Server configuration or deselect to disable the Java Method Server.
<b>ACS</b>	
<b>Documentum Server</b>	The list of Documentum CM Servers that is associated with the Java Method Server configuration.  A Java Method Server configuration can be associated with one or more Documentum CM Servers. <i>OpenText Documentum Content Management - Server and Server Extensions Installation Guide (EDCSY250400-IGD)</i> provides more information about installing multiple Documentum CM Servers, Java Method Servers, and the supported Java Method Server failover configurations.

Field	Description
<b>Documentum Server location</b>	<p>Specifies whether the Java Method Server is associated with a Documentum CM Server that is remote. Valid values are:</p> <ul style="list-style-type: none"> <li>• Java Method Server for primary Documentum Server: The Accelerated Content Services server is local.</li> <li>• Java Method Server for secondary (or additional) Documentum Server: The Accelerated Content Services server is remote.</li> </ul>
<b>Add</b>	<p>Click <b>Add</b> to add and associate a Documentum CM Server with the Java Method Server configuration.</p> <p>The Servlet URL Editor page displays. Select the Documentum CM Server and intended purpose, as described in <a href="#">“Adding or modifying Accelerated Content Services” on page 82</a>.</p>
<b>Edit</b>	<p>Select the Documentum CM Server and click <b>Edit</b> to modify the Documentum CM Server associated with the Java Method Server configuration.</p> <p>The Servlet URL Editor page displays. Modify the intended purpose, as described in <a href="#">“Adding or modifying Accelerated Content Services” on page 82</a>.</p>
<b>Remove</b>	<p>Select the Documentum CM Server and click <b>Remove</b> to remove the Documentum CM Server from the Java Method Server configuration.</p>
<b>Java Method Server Servlet URLs</b>	
<b>Name</b>	The name of the Java servlet.
<b>URL</b>	The location of the Java servlet.

### 3.7.3 Adding or modifying Accelerated Content Services

**To add or modify Accelerated Content Services server:**

1. Log in to the repository for which you want to create the Java Method Server configuration.
2. Select **Administration > Basic Configuration > Java Method Servers**.
3. In the **Java Method Server Configuration** page, select the Java Method Server configuration you want to modify, then select **View > Properties > Info** or right-click the Java Method Server configuration object and select **Properties**.
4. In the **Java Method Server Configuration Properties** page, do one of the following:
  - Click **Add** to associate a Documentum CM Server with the Java Method Server.
  - Select a Documentum CM Server and click **Edit** to modify the failover behavior for the Java Method Server.
5. Type the Documentum CM Server and Java Method Server failover information, as described in “[Accelerated Content Services server information](#)” on page 82.

**Table 3-15: Accelerated Content Services server information**

Field	Description
<b>Documentum Server</b>	The name of the Documentum CM Server associated with the Java Method Server.  To add a Documentum CM Server, select the Documentum CM Server from the drop-down list.  The drop-down list displays Documentum CM Server that were previously installed on the host machine using the Documentum CM Server configuration program. <i>OpenText Documentum Content Management - Server and Server Extensions Installation Guide (EDCSY250400-IGD)</i> provides more information about installing multiple Documentum CM Servers, Java Method Servers, and the supported Java Method Server failover configurations.

Field	Description
<b>Documentum Server location</b>	Specifies whether the Java Method Server is associated with a Documentum CM Server that is remote. Valid values are: <ul style="list-style-type: none"> <li>• Java Method Server for primary Documentum Server: The Accelerated Content Services is local.</li> <li>• Java Method Server for secondary (or additional) Documentum Server: The Accelerated Content Services is remote.</li> </ul>

### 3.7.4 Viewing active Java Method Server

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

**To display all active Java Method Server:**

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 is displayed with the information described in “[Active Java Method Server information](#)” on page 83.

To reset the information on the **Active Java Methods Servers List** page, click **Refresh**.

**Table 3-16: Active Java Method Server information**

Field	Description
<b>Associated Content Server</b>	The Documentum CM Server with which the Java Method Server cache is associated.
<b>Last Refreshed Time</b>	The last time the Documentum CM Server Java Method Server cache was reset.
<b>Incremental Wait Time on Failure</b>	The time Documentum CM Server waits before contacting the Java Method Server, if the Java Method Server fails to respond.  The wait time is doubled each time the Java Method Server fails to respond until the maximum wait time is reached.
<b>Maximum Wait Time on Failure</b>	The maximum wait time Documentum CM Server keeps trying to contact the Java Method Server, if the Java Method Server fails to respond.

Field	Description
<b>Java Method Server in Use</b>	The name of the active Java method server that was used last time.
<b>Java Method Servers associated with the Documentum Server</b>	
<b>Name</b>	The name of the Java Method Server configuration object.
<b>Is Enabled</b>	Specifies whether the Java method server is enabled or disabled.
<b>Status</b>	The current status of the Java Method Server configuration object.
<b>Documentum Server location</b>	Specifies whether the Java Method Server is associated with a Documentum CM Server that is remote. Valid values are: <ul style="list-style-type: none"> <li>• Java Method Server for primary Documentum Server: The Accelerated Content Services is local.</li> <li>• Java Method Server for secondary (or additional) Documentum Server: The Accelerated Content Services is remote.</li> </ul>
<b>Last Failure Time</b>	The last time the Java Method Server failed to respond.
<b>Next Retry Time</b>	The next time the Documentum CM Server tries to contact the Java Method Server, if the Java Method Server fails to respond.
<b>Failure Count</b>	The number of times the Java Method Server failed to respond.

### 3.7.5 Viewing and modifying Java Method Server HA configuration

Only users with superuser privileges can modify Java Method Server HA configurations.

**To modify Java Method Server HA configuration:**

1. Log in to the repository for which you want to modify the Java Method Server HA configuration.
2. Select **Administration > Basic Configuration > Java Method Servers**.
3. In the **Java Method Server Configuration** page, select the server configuration object you want to modify, then select **View > JMS HA Configuration** or right-click the server configuration object and select **JMS HA Configuration**.
4. In the **Java Method Server HA Configuration Properties** page, view or modify the information for the Java Method Server HA configuration, as described in “[Associated Java Method Server objects](#)” on page 85.

**Table 3-17: Associated Java Method Server objects**

<b>Field</b>	<b>Description</b>
<b>JMS Config Name</b>	The list of Java Method Server objects associated with the server configuration object.  A server configuration object can be associated with more than one Java Method Server configuration object.
<b>JMS Config ID</b>	The object ID of Java Method Server object associated with the server configuration object.
<b>JMS Mode</b>	The mode of Java Method Server object associated with the server configuration object. Valid values are: <ul style="list-style-type: none"> <li>• Load Balancing</li> <li>• Failover</li> <li>• Load Balancing &amp; Failover</li> </ul>
<b>Add</b>	Click <b>Add</b> to add and associate a Java Method Server object with the server configuration object.
<b>Edit</b>	Select the Java Method Server object and click <b>Edit</b> to modify the Java Method Server object associated with the server configuration object.
<b>Remove</b>	Select the Java Method Server object and click <b>Remove</b> to remove the Java Method Server object associated with the server configuration object.



**Note:** At least one Java Method Server object associated with the server configuration object must have the Java Method Server Mode as **Load Balancing** or **Load Balancing & Failover**.

### 3.7.6 Adding or removing associated Java Method Server objects

Use the Java Method Server page to add or remove Java Method Server objects that are associated with a server configuration object.

#### To add or remove associated Java Method Server objects:

1. Log in to the repository for which you want to create the Java Method Server configuration.
2. Select **Administration > Basic Configuration > Java Method Servers**.
3. In the **Java Method Server Configuration** page, select the server configuration object you want to modify, then select **View > JMS HA Configuration** or right-click the server configuration object and select **JMS HA Configuration**.
4. In the **Java Method Server HA Configuration Properties** page, do one of the following:
  - Click **Add** to associate a Java Method Server object with the server configuration object.
  - Select the Java Method Server object and click **Remove** to remove the Java Method Server object associated with the server configuration object.
5. In the **Associated Java Method Server** page, select the Java Method Server object and the corresponding mode, as described in “[Java Method Server objects and mode](#)” on page 86.

**Table 3-18: Java Method Server objects and mode**

Field	Description
JMS Config Name	Select the Java Method Server configuration object from the list of entries.
JMS Config ID	The object ID corresponding to the Java Method Server object will be displayed.
JMS Mode	The mode of Java Method Server object associated with the server configuration object. Valid values are: <ul style="list-style-type: none"><li>• Load Balancing</li><li>• Failover</li><li>• Load Balancing &amp; Failover</li></ul>

### 3.7.7 Viewing Java Method Server HA status

The status of all Java Method Server instances is displayed on the Java Method Server HA status page.

#### To view Java Method Server HA status:

1. Log in to the repository and select **Administration > Basic Configuration > Java Method Servers**.
2. Select **View > JMS HA Status** or right-click the server configuration object and select **JMS HA Status**.

The **Java Method Server HA Status** page is displayed with the information, as described in “[Java Method Server HA status](#)” on page 87.

To refresh the information on the **Java Method Server HA Status** page, click **Refresh**.

To refresh the Java Method server HA configuration with default values, click **Refresh Default**.

**Table 3-19: Java Method Server HA status**

Field	Description
<b>JMS Config ID</b>	The object ID of the Java Method Server configuration object.
<b>Status</b>	The status of the Java Method Server configuration object.
<b>Downtime</b>	The downtime of the Java Method Server configuration object.

## 3.8 LDAP servers

An Lightweight Directory Access Protocol (LDAP) directory server is a third-party product that maintains information about users and groups. Documentum CM 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. Documentum CM 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 Documentum CM 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 Documentum CM 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.

### 3.8.1 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 Documentum CM 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*. “[LDAP Server Configuration page properties](#)” on page 89 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 3-20: LDAP Server Configuration page properties**

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

### 3.8.2 Adding or modifying LDAP server configurations

When adding an LDAP directory server to an existing OpenText Documentum CM 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 OpenText Documentum CM 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” on page 91](#).
4. Click the **Sync & Authentication** tab and enter or modify the information on the **LDAP Server Configuration - Sync & Authentication** page, as described in [“LDAP Server Sync & Authentication properties” on page 94](#).
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” on page 95](#).
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” on page 97](#).
7. Click **Finish** when you have completed configuring the new LDAP server.

Documentum CM Server creates an `ldap<objectID>.cnt` password when you create the LDAP configuration object. If you have more than one Documentum CM Server associated with the repository, the password file must be copied to each Documentum CM Server in the environment or authentication fails.

When you want to create new `dm_ldap_config` object other than the one already created, you must manually provide full access permission to the MSA user to access the new `.cnt` file generated at `C:\Documentum\dba\config\testenv\`. Otherwise, it results in the access denied error when you run the LDAP synchronization job using the new LDAP configuration object. This is because, Windows does not allow default user permissions on a new file or folder.

### 3.8.2.1 LDAP Server Configuration properties

The following table describes the properties on the Info tab of the LDAP Server Configuration page. The properties apply to new and existing LDAP configuration objects.

**Table 3-21: LDAP Server Configuration Properties properties**

Field	Description
<b>Name</b>	The name of the new LDAP configuration object.  This field is read-only if you are viewing or modifying the LDAP configuration object.
<b>Status</b>	Select the Enable this LDAP Configuration check box to enable the LDAP configuration.
<b>Directory Type</b>	Refer to the Release Notes for your version of Documentum CM Server to see which LDAP server versions are supported.  Options are: <ul style="list-style-type: none"> <li>• Sun One/Netscape/iPlanet Directory Server (default)</li> <li>• Microsoft Active Directory</li> <li>• Microsoft ADAM</li> <li>• Oracle Internet Directory Server</li> <li>• IBM Directory Server</li> <li>• Novell eDirectory</li> </ul>
<b>Hostname / IP Address</b>	The name of the host on which the LDAP directory server is running. <p> <b>Warning</b></p> <p>Starting from the 7.0 release, use only the host name and not the IP address. However, you can use both the host name and IP address in pre-7.0 releases.</p>
<b>Port</b>	The port number where the LDAP directory server is listening for requests.  The default is 389.
<b>Binding Name</b>	The binding distinguished name used to authenticate requests to the LDAP directory server by Documentum CM Server or the check password program.

Field	Description
<b>Binding Password</b>	<p>The binding distinguished password used to authenticate requests to the LDAP directory server by Documentum CM Server or the check password program.</p> <p>The Binding Password field only appears on the New LDAP Server Configuration - Info page.</p>
<b>Confirm Password</b>	<p>If adding a new LDAP server configuration, re-enter the binding password for verification.</p> <p>The Confirm Password field only appears on the New LDAP Server Configuration page.</p>
<b>Set</b>	<p>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.</p>
<b>Use SSL</b>	<p>Specifies whether SSL is used for authentication.</p>
<b>SSL Port</b>	<p>Specifies the SSL port. This option only displays when the <b>Use SSL</b> option is selected.</p> <p>Enter 636 for the SSL port value.</p>
<b>Certificate Location</b>	<p>Specifies the location of the LDAP certificate database. If you selected <b>Use SSL</b>, the default location for <i>.cer</i> is <i>ldapcertdb_loc</i>.</p> <p>For <i>.pem</i> certificate browse and manually select the location object. The location object is created with the pem certificate name.</p> <p>If you are using more than one LDAP server in SSL mode, you must store the LDAP certificates a single location, as described in <a href="#">"Using multiple LDAP servers in SSL mode" on page 105</a>.</p>
<b>Validate SSL Connection</b>	<p>If you selected <b>Use SSL</b>, click to validate that a secure connection can be established with the LDAP server on the specified port. If the validation fails, the system displays an error message and you cannot proceed further until valid information is provided.</p>

**Follow these manual steps for SSL validation for 6.5x and earlier Documentum CM 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 preceding 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%:

### 3.8.2.2 LDAP Server Sync & Authentication properties

The following table 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 3-22: LDAP Server Sync & Authentication properties**

Field	Description
<b>Import</b>	Specifies how users and groups are imported. Available options are: <ul style="list-style-type: none"> <li>• Users and groups (default)</li> <li>• Users only</li> <li>• Groups &amp; member users</li> </ul>
<b>Synchronize Nested Groups in the repository</b>	Select to synchronize the nested groups in the repository.   <b>Note:</b> This option is enabled only if Import field has the value <b>Users and groups</b> or <b>Groups &amp; member users</b> . This option is disabled if you select <b>Users only</b> for Import field.
<b>Sync Type</b>	Specifies how users and groups are synchronized. Available options are: <ul style="list-style-type: none"> <li>• Full: Import all based on user/group mappings (default)</li> <li>• Incremental: Import only new or updated user/groups/members</li> </ul> If <b>Groups and member users</b> 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.
<b>Deleted Users</b>	Specifies whether deleted user accounts are marked inactive. Available options are: <ul style="list-style-type: none"> <li>• set to inactive (default)</li> <li>• unchanged</li> </ul>
<b>Update Names</b>	Select to <b>Update user names in repository</b> or <b>Update group names in repository</b> .  The Update group names in repository check box is not enabled if Users Only is selected in the Import field.
<b>User Type</b>	Select a user type. The default is <i>dm_user</i> .

Field	Description
<b>Bind to User DN</b>	Options are: <ul style="list-style-type: none"> <li>• <i>Search for DN in directory using user's login name</i></li> <li>• <i>Use DN stored with user record in repository (default)</i></li> </ul>
<b>External Password Check</b>	Select to use external password check to authenticate users to directory.

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.

### 3.8.2.3 LDAP Server mapping properties

The following table describes the properties on the Mapping tab of the LDAP Server Configuration page. The properties apply to new and existing LDAP configuration objects.

**Table 3-23: LDAP Server mapping properties**

Field	Description
<b>User Object Class</b>	Type the user object class to use for searching the users in the directory server.
<b>User Search Base</b>	Type the user search base. This is the point in the LDAP tree where searches for users start. For example:  cn=Users,ou=Server,dc=sds,dc=inengvm1llc,dc=corp,dc=test,dc=com.
<b>User Search Filter</b>	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=*

Field	Description
<b>Search Builder</b>	Click to access the Search Builder page. This page enables you to build and test a user search filter. When finished, the User Search Filter field is populated with the resulting filter.
<b>Group Object Class</b>	<p>Type the group object class to use for searching the groups in the directory server. Typical values are:</p> <ul style="list-style-type: none"> <li>• For Netscape and Oracle LDAP servers: groupOfUniqueNames</li> <li>• For Microsoft Active Directory: group</li> </ul>
<b>Group Search Base</b>	<p>Type the group search base. This is the point in the LDAP tree where searches for groups start. For example:</p> <p>cn=Groups,ou=Server,dc=sds,dc=inengvm1llc,dc=corp,dc=test,dc=com</p>
<b>Group Search Filter</b>	Type the group search filter. This is the name of the filter used to make an LDAP group search more specific. The typical filter is cn=*
<b>Search Builder</b>	Click to access the Search Builder page. This page enables you to build and test a group search filter. When finished, the Group Search Filter field is populated with the resulting filter.
<b>Property Mapping</b>	When a new configuration is added, this table populates with the mandatory mapping attributes. The mappings are dependent upon the directory type. This table defines the pre-populated attributes and their mappings. All mapping types are LDAP Attribute.
<b>Add</b>	Click to access the Map Property page to add an attribute. Select an attribute and then select the LDAP attribute to which the attribute maps or type in a custom value.
<b>Edit</b>	Select an attribute and then click Edit to access the Map Property page. On the Map Property page, edit the attribute properties.
<b>Delete</b>	Select an attribute and then click Delete to remove an attribute. The system displays the Deletion Confirmation page.
<b>Repository Property</b>	Displays the repository property that is the target of the mapping.

Field	Description
Type	Identifies the source of the property: User or Group.
Map To	Displays which attributes on LDAP that the property is mapped to.
Map Type	Identifies the type of data: LDAP attribute, expressions, or a fixed constant.
Mandatory	<p>Indicates if the mapping is mandatory for the attribute.</p> <p>Documentum CM Server requires three properties to be defined for a user and one property to be defined for a group. The mandatory properties are:</p> <ul style="list-style-type: none"> <li>• user_name</li> <li>• user_login_name</li> <li>• group_name</li> </ul> <p>You can change the defaults, but you must provide some value or mapping for these properties. Users cannot be saved to the repository without values for these three properties, nor can a group be saved to the repository without a group name.</p>

### 3.8.2.4 LDAP Server failover properties

The following table describes the properties on the Failover tab of the LDAP Server Configuration page. The properties apply to new and existing LDAP configuration objects.

**Table 3-24: LDAP Server failover properties**

Field	Description
Failover Settings	Use this section to enter settings for the primary LDAP server.
Retry Count	<p>The number of times Documentum CM Server tries to connect to the primary LDAP server before failing over to a designated secondary LDAP server. The default is 3.</p> <p>If the retry count value is set to 0, Documentum CM Server immediately reports that it failed to contact the primary LDAP directory server.</p>

Field	Description
<b>Retry Interval</b>	<p>Enter an interval number and select a duration (seconds, minutes, or hours) between retries. The default is at 3 seconds.</p> <p>Documentum CM 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.</p>
<b>Reconnect</b>	<p>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.</p> <p>The default is set at 5 minutes.</p>
<b>Secondary LDAP Servers</b>	<p>Specifies secondary LDAP servers.</p> <ul style="list-style-type: none"> <li>• To add a new secondary LDAP server, click <b>Add</b>. The Secondary LDAP Server page is displayed.</li> <li>• To modify an existing secondary LDAP server, select the check box next to the name and click <b>Edit</b>. The Secondary LDAP Server page is displayed.</li> <li>• To delete an existing secondary LDAP server, select the check box next to the name and click <b>Delete</b>.</li> <li>• To reorder the list of LDAP servers, click <b>Move Up</b> or <b>Move Down</b>.</li> </ul>
<b>Name</b>	Name of the secondary LDAP server.
<b>Hostname</b>	The name of the host on which the secondary LDAP directory server is running.
<b>Port</b>	The port information.
<b>SSL Port</b>	The SSL port number.

### 3.8.3 Mapping LDAP Servers

LDAP directory servers allow you to define attribute values for user and group entries in the directory server. Documentum CM 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 `given_name` 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 preceding expression resolves to `smith_p@company.com`. The 1 at the end of given name 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.

The following table 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 3-25: Netscape iPlanet, Oracle Internet Directory Server, and Microsoft Active Directory example**

DM attribute	DM type	LDAP attribute	Type
<code>user_name</code>	<code>dm_user</code>	<code>cn</code>	A
<code>user_login_name</code>	<code>dm_user</code>	<code>uid</code>	A

### 3.8.3.1 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 property lengths apply to the mappings. For example, the mapping string for `user_name` must resolve to 32 characters or less.

### 3.8.3.2 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.

### 3.8.3.3 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**.

### 3.8.4 Configuring secondary LDAP servers

You can configure Documentum CM 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 Documentum CM 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 the following table:

**Table 3-26: Secondary LDAP Server page properties**

<b>Field</b>	<b>Description</b>
<b>Name</b>	Enter the name of the secondary LDAP server.
<b>Hostname / IP Address</b>	Type the name of the host on which the secondary LDAP directory server is running.
<b>Port</b>	The port information is copied from the primary LDAP server.
<b>Binding Name</b>	The binding name is copied from the primary LDAP server.
<b>Binding Password</b>	Type the binding distinguished password used to authenticate requests to the secondary LDAP directory server by Documentum CM Server or the check password program.
<b>Confirm Password</b>	Re-enter the binding password for verification.
<b>Bind to User DN</b>	The bind to user DN information is copied from the primary LDAP server.
<b>Use SSL</b>	The SSL information is copied from the primary LDAP server.
<b>SSL Port</b>	The SSL port number is copied from the primary LDAP server.
<b>Certificate Location</b>	The certificate location is copied from the primary LDAP server.

### 3.8.5 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 Documentum CM 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.

### 3.8.6 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.

### 3.8.7 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.

### 3.8.8 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 Documentum CM Server's server configuration object, the Documentum CM 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 Documentum CM 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.

### **3.8.9 Using LDAP directory servers with multiple Documentum CM Servers**

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

**To enable LDAP authentication with multiple Documentum CM Servers:**

1. Using Documentum Administrator, connect to one of the nonprimary Documentum CM 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 Documentum CM Server.

### 3.8.10 LDAP proxy server support

Documentum CM 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.

## 3.9 LDAP Certificate Database Management

The LDAP Certificate Database Management system enables administrators to:

- Import certificates into the LDAP certificate database on the Documentum CM 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.

### 3.9.1 Viewing LDAP certificates

Documentum CM 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.

### 3.9.2 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.

### 3.9.3 Using multiple LDAP servers in SSL mode

Documentum CM 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” on page 105](#).
3. Modify the certification location field for each LDAP server configuration that uses SSL to point to the same certificate database location.

By default, Documentum CM Server assigns the file path that is specified in the *ldapcertdb\_loc* object.

### 3.9.4 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 Documentum CM Server, restart the method server, then import the new certificates, as described in “[Importing LDAP certificates](#)” on page 105.

# Chapter 4

## Distributed configurations

### 4.1 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 OpenText Documentum CM web clients. For example, a OpenText Documentum CM 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 Accelerated Content Services configuration objects. The server configuration objects and Accelerated Content Services configuration objects contain information defining the proximity of a Documentum CM Server or Accelerated Content Services server to the network location. Documentum CM Server uses the information in the server configuration objects and Accelerated Content Services 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 Foundation Java API 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 Foundation Java API 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.

*OpenText Documentum Content Management - Server and Server Extensions Installation Guide (EDCSY250400-IGD)* provides more information about network locations.

### 4.1.1 Creating, viewing, or modifying network locations

Network locations should be created in the global registry repository that is defined when Foundation Java API is installed on the Documentum Administrator host. You must have superuser privileges in the global registry repository to create network locations. *OpenText Documentum Content Management - Server and Server Extensions Installation Guide (EDCSY250400-IGD)* 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 Foundation Java API 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 “[Network location properties](#)” on page 109.
5. Click **OK** to save your changes.

**Table 4-1: Network location properties**

<b>Field</b>	<b>Description</b>
<b>Network Location Identifier</b>	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.
<b>Subject</b>	A description of the network location.
<b>Default Network Location</b>	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 check box selected, that network location is used automatically and the user does not see the list.
<b>Network Location Name</b>	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 OpenText Documentum CM 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.

Field	Description
<b>IP Address Ranges</b>	<p>The IP address range identified by the network location. Each range must conform to standard IP address conventions. A network location may have multiple IP address ranges. It is recommended that each IP address is mapped to a single network location, but if an IP address maps to multiple physical locations, you may need to map that address to multiple network locations.</p> <p>Type the IP address in one of the following formats:</p> <ul style="list-style-type: none"> <li>• IPv4 address range can be entered by separating the two IP address with a hyphen(-). For example: x.x.x.x-x.x.x.x where x is from 0 to 255.</li> <li>• 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 or x:x:x::y (ipv6-address/prefix-length) where the x's are the hexadecimal values of the eight 16-bit pieces of the address and y is a decimal value specifying how many of the leftmost contiguous bits of the address comprise the prefix.</li> </ul>

### 4.1.2 Copying network locations

To save time retying 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 Foundation Java API 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.

### 4.1.3 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 OpenText Documentum Content Management (CM) Branch Office Caching Services or Accelerated Content Services 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, Accelerated Content Services configuration objects, Branch Office Caching Services configuration objects, and Branch Office Caching Services 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 Foundation Java API 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** 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, Accelerated Content Services configuration objects, Branch Office Caching Services configuration objects, and Branch Office Caching Services caching jobs in the current repository and any other repositories.

## 4.2 Accelerated Content Services servers

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

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

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

*OpenText Documentum Content Management - Server and Server Extensions Installation Guide (EDCSY250400-IGD)* provides information on modifying the acs.properties file and additional information about the Accelerated Content Services server.

The Accelerated Content Services server is configured on the Accelerated Content Services servers configuration page that can be accessed in the **Administration > Distributed Content Configuration > ACS Servers** node. See “[Accelerated Content Services server configuration](#)” on page 113.

**Table 4-2: Accelerated Content Services server configuration**

<b>Field</b>	<b>Description</b>
<b>Name</b>	The name that is assigned to the Accelerated Content Services server during the Documentum CM Server installation. The name cannot be modified.
<b>Documentum Server</b>	The name of the Documentum CM Server the Accelerated Content Services server is associated with.
<b>Content Access</b>	Specifies how the Accelerated Content Services server can access content. Valid values are: <ul style="list-style-type: none"> <li>• <i>Access all stores</i>: The Accelerated Content Services server can access all stores that are connected to the Documentum CM Server.</li> <li>• <i>Access local stores only</i>: The Accelerated Content Services 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.</li> <li>• <i>None (disabled)</i>: The Accelerated Content Services server is disabled.</li> </ul>
<b>Projections &amp; Stores from</b>	Specifies the connection broker projections, network locations, and local stores information for the Accelerated Content Services server.
<b>Description</b>	A description of the Accelerated Content Services server.
<b>Dormancy Status</b>	The current dormancy status of the Accelerated Content Services server. Valid values are: <ul style="list-style-type: none"> <li>• <b>Dormant</b></li> <li>• <b>Active</b></li> </ul> <p> <b>Note:</b> The Dormancy Status column is only visible for 7.0 and later versions of repositories.</p>

## 4.2.1 Viewing or modifying the Accelerated Content Services server configuration properties

1. Connect as a superuser to the repository in which you want to view or modify the Accelerated Content Services server.
2. Select **Administration > Configuration > ACS Servers**.  
The **ACS Servers Configurations** list page appears.
3. Select the Accelerated Content Services 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 “[Accelerated Content Services server configuration properties](#)” on page 114.
5. Click the **Projections & Stores** tab to view or modify the connection broker projections, network locations, and local stores information for the Accelerated Content Services server, as described in “[Viewing or modifying the Accelerated Content Services projections and stores](#)” on page 116.
6. Click **OK** to save your changes.
7. Restart the Accelerated Content Services server.

The Accelerated Content Services server runs in the same servlet container as the 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.

*OpenText Documentum Content Management - Server and Server Extensions Installation Guide (EDCSY250400-IGD)* provides instructions on stopping and starting the Java method server.

**Table 4-3: Accelerated Content Services server configuration properties**

Field	Description
<b>ACS Server Configuration</b>	
<b>Name</b>	The name that is assigned to the Accelerated Content Services server during the Documentum CM Server installation. The name cannot be modified.
<b>ACS</b>	The name of the Documentum CM Server the Accelerated Content Services server is associated with.
<b>Description</b>	A description of the Accelerated Content Services server.

Field	Description
<b>ACS Server Version</b>	<p>The major and minor version of the Accelerated Content Services server.</p> <p>The Accelerated Content Services server version indicates the underlying repository version.</p> <p>Valid values:</p> <ul style="list-style-type: none"> <li>• 2.1 - Specifies that the Accelerated Content Services server is part of a OpenText Documentum CM version 6.5 SPx repository.</li> <li>• 2.2 - Specifies that the Accelerated Content Services server is part of a OpenText Documentum CM version 6.6 to 6.6 (Patch 21) repository.</li> <li>• 2.3 - Specifies that the Accelerated Content Services server is part of a OpenText Documentum CM version 6.6 (Patch 22) to the latest version.</li> </ul>
<b>Dormancy Status</b>	<p>Indicates the dormancy status of Accelerated Content Services server.</p> <p> <b>Note:</b> The Dormancy Status label is only visible for 7.0 and later versions of repositories.</p>
<b>Content Access</b>	<p>Specifies how the Accelerated Content Services server can access content. Valid values are:</p> <ul style="list-style-type: none"> <li>• <i>Access all stores</i>: The Accelerated Content Services server can access all stores that are connected to the Documentum CM Server.</li> <li>• <i>Access local stores only</i>: The Accelerated Content Services server can read content from local file stores in the repository.</li> <li>• <i>None (disabled)</i>: The Accelerated Content Services server is disabled.</li> </ul>
<b>ACS Server Connections</b>	
<b>Protocol</b>	<p>The protocol the Accelerated Content Services server uses. Valid values are http and https. Click <b>Add</b> to add a protocol, or select a protocol from the list and click <b>Edit</b> to modify it or <b>Delete</b> to remove the protocol.</p>

Field	Description
<b>Base URL</b>	The base URL for the Accelerated Content Services server. The base URL requires the following format: <code>&lt;protocol&gt;://&lt;host&gt;:&lt;port&gt;/ACS/servlet/ACS</code>

## 4.2.2 Viewing or modifying the Accelerated Content Services projections and stores

1. Connect with superuser privileges to the repository in which you want to view or modify the Accelerated Content Services projections and stores.
2. Select **Administration > Configuration > ACS Servers**.  
The **ACS Servers Configurations Properties** list page appears.
3. Select the Accelerated Content Services 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 [“Accelerated Content Services projections and stores properties” on page 117](#).
6. Click **OK** to save your changes.
7. Restart the Accelerated Content Services server.

The Accelerated Content Services server runs in the same servlet container as the 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.

*OpenText Documentum Content Management - Server and Server Extensions Installation Guide (EDCSY250400-IGD)* provides instructions on stopping and starting the Java method server.

**Table 4-4: Accelerated Content Services projections and stores properties**

<b>Field</b>	<b>Description</b>
<b>Source</b>	<p>Specifies where to use projections and stores for the Accelerated Content Services server. Valid values are:</p> <ul style="list-style-type: none"> <li>• <b>ACS:</b> The Accelerated Content Services server uses the connection broker projections, network locations, and local stores already configured for the Accelerated Content Services.</li> <li>• <b>Settings entered here:</b> You must enter the Accelerated Content Services server uses connection brokers, network locations, and near stores manually.</li> </ul> <p>If you select this option, an <b>Add</b> button displays in the Connection Broker Projections, Network Location Projections, and Local Stores sections.</p>
<b>Connection Broker Projections</b>	
<b>Target Host</b>	<p>The host name of the server that hosts the connection broker.</p> <p>Click <b>Add</b> to add a target host, or select a host from the list and click <b>Delete</b> to remove the host.</p> <p>The connection broker is a process that provides client sessions with server connection information. Each Accelerated Content Services server broadcasts information to connection brokers at regular intervals.</p>
<b>Port</b>	The port number on which the connection broker is listening.
<b>Enabled</b>	Enables projections to the connection broker.
<b>Network Location Projections</b>	
<b>Network Location</b>	<p>Specifies a network location in the global registry of the Documentum CM Server host.</p> <p>Click <b>Add</b> to add a network location, or select a location from the list and click <b>Delete</b> to remove the location.</p> <p>Network locations identify locations on a network, and, optionally, a range of IP addresses, from which users connect to the web clients.</p>
<b>Display Name</b>	A name that describes the network location.

Field	Description
<b>Proximity</b>	The proximity value for the network location.
<b>Enabled</b>	Enables projection to that network location.
<b>Local Stores</b>	
<b>Local Store</b>	A local store.  Click <b>Add</b> to add a store, or select a store from the list and click <b>Delete</b> to remove the store.  Local stores are defined as near to the Accelerated Content Services server.
<b>Type</b>	Specifies the storage type associated with the local store. This property cannot be modified.

### 4.2.3 Designating connection brokers for an Accelerated Content Services server

To designate a connection broker for an Accelerated Content Services 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 Accelerated Content Services 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 “[Accelerated Content Services connection broker projections properties](#)” on page 119.
5. Click **OK**.
6. Restart the Accelerated Content Services server.

The Accelerated Content Services server runs in the same servlet container as the 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.

*OpenText Documentum Content Management - Server and Server Extensions Installation Guide (EDCSY250400-IGD)* provides instructions on stopping and starting the Java method server.

**Table 4-5: Accelerated Content Services connection broker projections properties**

Field	Description
<b>Source</b>	<p>Specifies where to use projections for the Accelerated Content Services server. Valid values are:</p> <ul style="list-style-type: none"> <li>• <b>ACS:</b> The Accelerated Content Services server uses the connection broker projections, network locations, and local stores already configured for the Accelerated Content Services server.</li> <li>• <b>Settings entered here:</b> Select this option to designate connection broker projections.</li> </ul> <p>If you select this option, an <b>Add</b> button displays in the Connection Broker Projections, Network Location Projections, and Local Stores sections.</p>
<b>Connection Broker Projections</b>	
<b>Target Host</b>	<p>The host name of the server that hosts the connection broker.</p> <p>Click <b>Add</b> to add a target host, or select a host from the list and click <b>Delete</b> to remove the host.</p> <p>The connection broker is a process that provides client sessions with server connection information. Each Accelerated Content Services server broadcasts information to connection brokers at regular intervals.</p>
<b>Port</b>	The port number on which the connection broker is listening.
<b>Enabled</b>	Enables projections to the connection broker.

#### 4.2.4 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 Foundation Java API 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.

### 4.3 Branch Office Caching Services servers

Branch Office Caching Services 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 Branch Office Caching Services server can serve content from multiple repositories.

Branch Office Caching Services servers communicate only with Accelerated Content Services servers and OpenText™ Documentum™ Content Management Messaging Service servers, but not directly with Documentum CM Servers. Every Branch Office Caching Services server for OpenText Documentum CM 6 or later repositories is associated with a `dm_bocs_config` object. The installation program for the Branch Office Caching Services server does not create the object at installation time. The Branch Office Caching Services server must be added manually, using the properties on the Branch Office Caching Services servers configuration page. All Branch Office Caching Services configuration objects for OpenText Documentum CM 6 or later repositories reside in the global registry in the `/System/BocsConfig` folder.

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

### 4.3.1 Creating, viewing, or modifying Branch Office Caching Services servers

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

**To create, view, or modify Branch Office Caching Services servers:**

1. Connect to the global registry associated with the Foundation Java API 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 Branch Office Caching Services server configuration object.
  - Select a Branch Office Caching Services server configuration object and then select **View > Properties > Info** to view or modify a Branch Office Caching Services server configuration object.
4. Type or modify the information on the Info and Security tabs of the **New BOCS Server Configuration** or **BOCS Server Configuration** page, as described in “Branch Office Caching Services server properties” on page 121 and “Setting Branch Office Caching Services server security” on page 124.
5. Click **Finish** or **OK** to save your changes.

**Table 4-6: Branch Office Caching Services server properties**

Field	Description
<b>BOCS Server Configuration Info</b>	
<b>Name</b>	The object name of the Branch Office Caching Services server.  The object name cannot be modified for existing Branch Office Caching Services server configuration objects.
<b>Description</b>	Description of the Branch Office Caching Services server.

Field	Description
<b>BOCS Server Version</b>	<p>A numeric string that identifies the set of Distributed Content features with which the Branch Office Caching Services server is compatible. In some cases, a set of features spans multiple product versions. Valid values are:</p> <ul style="list-style-type: none"> <li>• 1 - The Content Access options are limited to Read Only and None (disabled).</li> <li>• 2.1 - Compatible with Documentum CM Server version 6.5 SPx.</li> <li>• 2.2 - Compatible with Documentum CM Server version 6.6 to 6.6 Patch 21.</li> <li>• 2.3 - Compatible with Documentum CM Server versions 6.6 Patch 22 to the latest version. This value is only valid if the actual version of the installed Branch Office Caching Services server is from 6.6 Patch 22 to the latest version. This is the default value.</li> </ul>
<b>Content Access</b>	<p>Select an access type, as follows:</p> <ul style="list-style-type: none"> <li>• <b>Read and synchronous write:</b> Select this option for the Branch Office Caching Services server to support read and synchronous write.</li> <li>• <b>Read, synchronous, and asynchronous write:</b> Select this option for the Branch Office Caching Services server to support read, synchronous write, and asynchronous write.</li> <li>• <b>None (disabled):</b> The Branch Office Caching Services server is disabled.</li> </ul>
<b>Network Locations</b>	<p>Network locations served by the Branch Office Caching Services server.</p> <p>Click <b>Select</b> to access the Choose a Network Location page to select network locations.</p>

Field	Description
<b>Repositories</b>	<p>Select a repository from which to serve content, as follows:</p> <ul style="list-style-type: none"> <li>• <b>all repositories:</b> Content is served from all repositories.</li> <li>• <b>selected repositories only:</b> Serves content from all repositories that are specified on the Include list. Click <b>Edit</b> to add specific repositories.</li> <li>• <b>all except selected repositories:</b> Serves content from all repositories except the repositories that are specified in the Exclude list.</li> </ul> <p>Click the <b>Edit</b> link to add specific repositories to exclude.</p>
<b>Proxy URL</b>	<p>The Branch Office Caching Services proxy URL. The URL can contain up to 240 characters. The Branch Office Caching Services proxy URL is a message URL that only OpenText Documentum Content Management (CM) Messaging Service uses when Branch Office Caching Services is in push mode.</p>
<b>BOCS Server Connections</b>	
<b>Add</b>	<p>Click to add a protocol and base URL for the Branch Office Caching Services server.</p>
<b>Edit</b>	<p>Select a communication protocol and then click <b>Edit</b> to access the <b>BOCS Server Connection page</b> to edit a protocol and base URL for the Branch Office Caching Services server.</p>
<b>Delete</b>	<p>To delete a Branch Office Caching Services server protocol and base URL, select a communication protocol and then click <b>Delete</b>.</p>

Field	Description
<b>Protocol and Base URL</b>	The communication protocols used by the Branch Office Caching Services server to provide content to end users. The HTTP and HTTPS protocols are supported. The Base URL must be provided when the Branch Office Caching Services server is created. It is in the form:  <code>&lt;protocol&gt;://&lt;host&gt;:&lt;port&gt;/ACS/servlet/ACS</code> where <i>protocol</i> is http or https; <i>host</i> is the name of the computer on which the Branch Office Caching Services server is installed; and <i>port</i> is the port designated for communications during Branch Office Caching Services server installation.

### 4.3.2 Setting Branch Office Caching Services server security

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

The Branch Office Caching Services server configuration object in the global registry contains the public key information and generates an electronic signature for the Branch Office Caching Services server to use when contacting the Messaging Service server. When the Branch Office Caching Services server connects to the Messaging Service server in push or pull mode, it sends its electronic signature to Messaging Service where Messaging Service matches the electronic signature to the public key in the Branch Office Caching Services configuration object. If the Messaging Service server authenticates the Branch Office Caching Services electronic signature, the Branch Office Caching Services server can then push or pull its messages from or to the Messaging Service server respectively.

#### To set Branch Office Caching Services server security:

1. Connect to the global registry associated with the Foundation Java API 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 Branch Office Caching Services server configuration object. Type the Branch Office Caching Services server properties on the **Info** tab.
  - Select a Branch Office Caching Services server configuration object, then select **View > Properties > Info** to view or modify a Branch Office Caching Services server configuration object.

4. Click the **Security** tab and enter, view, or modify the security properties for the Branch Office Caching Services server, as described in “[Branch Office Caching Services server security properties](#)” on page 125.
5. Click **OK** to save changes.

**Table 4-7: Branch Office Caching Services server security properties**

Field	Description
<b>Pull Mode Enabled</b>	Specifies whether the Branch Office Caching Services server communicates with the Messaging Service server using the pull mode.  If this option is not selected, the Branch Office Caching Services server communicates with the Messaging Service server using the push mode.
<b>Public Key Installed</b>	Displays the last updated status for the public key.
<b>Upload Public Key File</b>	Click <b>Browse</b> to locate and install the public key file for the Branch Office Caching Services server for both the push and pull modes.

### 4.3.3 Setting Branch Office Caching Services server communication protocols

On the **BOCS Server Connection** page, set the communication protocols used by the Branch Office Caching Services 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 Branch Office Caching Services servers](#)” on page 121 provides the instructions.

**To set the Branch Office Caching Services 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 Branch Office Caching Services 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 Branch Office Caching Services server is installed; and *port* is the port

designated for communications during Branch Office Caching Services server installation.

4. Click **OK**.

#### 4.3.4 Deleting Branch Office Caching Services servers

Use the instructions in this section to delete Branch Office Caching Services server configuration objects from a global registry repository.

Deleting the configuration object does not uninstall the Branch Office Caching Services servers; they must be manually uninstalled from the hosts on which they are running. Without the configuration object, the Branch Office Caching Services server cannot provide content from this repository.

**To delete Branch Office Caching Services servers:**

1. Connect to the global registry known to Foundation Java API 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 Branch Office Caching Services 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 Branch Office Caching Services servers, select **Next** or **Finish**.

### 4.4 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 Accelerated Content Services is enabled for the repository and whether Branch Office Caching Services 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 Accelerated Content Services.

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 Accelerated Content Services. 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 check box 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 Branch Office Caching Services `acs.properties` file is set to *Required*.
- **Require BOCS to always encrypt content:** Select to encrypt content on Branch Office Caching Services. Content is not stored on Branch Office Caching Services if Branch Office Caching Services version does not support encryption or if the `encryption.mode` parameter in Branch Office Caching Services `acs.properties` file is set to *Disabled*.
- **Disable BOCS content encryption:** Select to not encrypt content on Branch Office Caching Services.

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.

## 4.5 Messaging server configuration

A Messaging Service server is an intermediary server that provides messaging services between an Accelerated Content Services or Branch Office Caching Services 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 earlier 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 Documentum CM 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 Messaging Service server configuration object, you must be connected to the repository known to Foundation Java API 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 OpenText Documentum CM 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 Foundation Java API 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 2.3 for Documentum CM Server 6.0 to the latest version.
- **Messaging:** Select to enable content transfer messaging to the Messaging Service server. This check box must be selected to enable asynchronous content transfer through Branch Office Caching Services and for predictive caching to work.

Clear the check box to disable content transfer messages to the Messaging Service server, even if the Messaging Service server is running.

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

- a. **Post URL:** Type the host name and port where to send messages to the Messaging Service server. This is a required field.
- b. **Consume URL:** Type the host name and port where Branch Office Caching Services servers in push or pull mode pick up messages from the Messaging Service server. If you do not have Branch Office Caching Services servers using the push or 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 retying 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 Foundation Java API 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 displays *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 5

## System reports

You can access all the system reports from **Administration > System Reports**.

To update the reports, go to the report and click **Refresh**. To export the reports, go to the report you want to export and click **Export Report**.

### 5.1 System overview report

The following tables describe the information on the **System Overview** report:

**Table 5-1: User information**

Field	Description
User	User name.

**Table 5-2: Report information**

Field	Description
Docbase Name	Repository name to which the user is connected.
Docbase Version	Repository version.
Projected Docbrokers	Projected connection broker name.
Report Date	Current date and time of the report.
Hostname	Host name of the Documentum CM Server host to which the user is connected.
Global Repository Name	Global repository name.

**Table 5-3: Server information**

Field	Description
Content Storage Services	Indicates if Content Storage Services is available.
Trusted Mode	Indicates if Trusted Content Services is available.
Content Intelligence Services	Indicates if Content Intelligence Services is available.

**Table 5-4: List of platform extensions information**

Field	Description
<b>BOCS Servers</b>	Number of Branch Office Caching Services servers associated with the repository.
<b>ACS Servers</b>	Number of Accelerated Content Services servers associated with the repository.
<b>BOCS Pre-caching</b>	Indicates if the repository is enabled to process precaching requests.
<b>DMS Servers</b>	Number of Messaging Service servers associated with the repository.

**Table 5-5: Product information**

Field	Description
<b>Collaborative Edition</b>	Indicates if Collaborative Edition is available.
<b>Physical Records Management</b>	Indicates if OpenText™ Documentum™ Content Management Physical Records Manager is available.
<b>Retention Policy Services</b>	Indicates if OpenText™ Documentum™ Content Management Retention Policy Services is available.
<b>Federated Records Services</b>	Indicates if Federated Records Services is available.
<b>Records Manager</b>	Indicates if OpenText™ Documentum™ Content Management Records Manager is available.

**Table 5-6: Distributed Content configuration information**

Field	Description
<b>BOCS Servers Configurations</b>	Indicates if Branch Office Caching Services server is installed and configured. Valid values are INSTALLED and NOT INSTALLED.

**Table 5-7: Storage information**

Field	Description
<b>STORAGE Snaplock Connector</b>	Indicates if STORAGE Snaplock Connector is available.

**Table 5-8: Content delivery information**

<b>Field</b>	<b>Description</b>
<b>IDS Administration</b>	Number of IDS administration.
<b>IDS Configurations</b>	Number of IDS configurations for a specific source and target configured for the repository.

**Table 5-9: OpenText Documentum Content Management (CM) Transformation Services information**

<b>Field</b>	<b>Description</b>
<b>Host 0</b>	Transformation Services component name that is integrated with Documentum CM Server to perform analysis and transformation activities.
<b>Transformations - Q1, Q2, Q3, Q4</b>	Number of renditions generated quarterly at any given Transformation Services instance.
<b>Listing File Store Details</b>	Indicates the total number of file stores and also provides the following details: <ul style="list-style-type: none"> <li>• <b>File Store Name</b></li> <li>• <b>Media Type</b></li> <li>• <b>Last Stored Time</b></li> <li>• <b>Store Type</b></li> <li>• <b>Active File Count</b></li> <li>• <b>Orphaned File Count</b></li> </ul>

**Table 5-10: Summary of users information**

<b>Field</b>	<b>Description</b>
<b>Summary of Users</b>	Total number of active and deactivated users.

## 5.2 User list report

Click **Administration > System Reports > User List** to view the detailed information of the user.

The report provides the following information:

- Object ID of the user.
- Name of the user.
- Email ID of the user.
- Date when the user was deactivated.

- Last date when the user performed a modification.
- Last time when the user logged in.
- Current state of the user.
- Expertise level of the user.
- Privileges of the user.
- Authentication mechanism of name and password of the user.
- Current roles of the user.

### 5.3 User activity report

Click **Administration > System Reports > User Activity** to view the roles of the user and documents owned by each user.

The report provides the following information:

- Object ID of the user.
- Name of the user.
- Number of documents owned by the user.
- Current roles of the user.
- Current extended roles of the user.

### 5.4 Transaction report

Click **Administration > System Reports > Transaction Report** to view the detailed report on transaction events that are enabled for tracking in Audit Trail.

The report provides the following information:

- ID of the Foundation Java API session.
- Name of the user.
- Name of the audited event.
- Description of the audited event.
- Time stamp of the audited event.
- Name of the audited object owner.

## 5.5 External transaction activity report

Click **Administration > System Reports > External Transaction Activity** to view the external transaction activity report information.

To generate the external transaction activity report, select the year for the **Quarterly Report** list and click **Generate Report**.

You can view the following information:

- Name of the user.
- Number of transactions performed by each user every quarter of the selected year.
- Total number of transactions performed by each user for all the quarters of the selected year.
- Total number of transactions performed by all users for the selected year.



**Note:** When you export the external transaction activity report, the CSV file name format is as follows:

Documentum External Transactions Summary - <repository name> - <transaction date>.csv

## 5.6 End user report

Click **Administration > System Reports > End User Report** to view the end user tracking information.

To generate a report, specify the details as described in the following table:

Field	Description
<b>Events</b>	Events registered for auditing. Valid values are: <ul style="list-style-type: none"> <li>• Default</li> <li>• DM_CONNECT</li> <li>• DM_LOGON_FAILURE</li> </ul>
<b>Region</b>	Geographical location of the user. The default value is ALL.
<b>Audit Dates</b>	Format of the date. Valid values are Local Time and UTC.
<b>From and Through</b>	Start and end time of the report.

To view the report, click **Generate Report**.

The report provides the following information:

- Name of the user.
- ID of the Foundation Java API session.
- Name of the audited event.
- Unique identifier for the Foundation Java API client and client name. The client name appears only if configured in Foundation Java API.
- IP address of the client machine from which the user is connected.
- Geographical location of the client machine from which the user is connected.
- Host name of the application server host to which the user is connected.
- Time stamp of the audited event.

## 5.7 Occasional user role report

Click **Administration > System Reports > Occasional User Role Report** to view all the session-related information of the occasional users that are part of the `dm_occasional_user_role` role.

The report provides the following information:

- ID of the Foundation Java API session.
- Name of the user.
- Start time of the user session.
- End time of the user session.

# Chapter 6

## User management

### 6.1 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 [“Users, groups, roles, and sessions” on page 137](#).

**Table 6-1: Users, groups, roles, and sessions**

Link	Description
<b>Users</b>	Accesses the Users page. From the Users page you can <ul style="list-style-type: none"><li>• Search for existing user accounts.</li><li>• Create, modify, and delete user accounts.</li><li>• View and assign group memberships for a particular user account.</li><li>• Change the home repository for particular user accounts.</li></ul> <a href="#">“Users” on page 138</a> provides more information about user accounts.
<b>Groups</b>	Accesses the Groups page. From the Groups page you can <ul style="list-style-type: none"><li>• Search for existing group accounts.</li><li>• Create, modify, and delete group accounts.</li><li>• View and reassign group a particular group account.</li></ul> <a href="#">“Groups” on page 155</a> provides more information about group accounts.

Link	Description
<b>Roles</b>	<p>Accesses the Roles page. From the Roles page you can</p> <ul style="list-style-type: none"><li>• Search for existing roles.</li><li>• Create, modify, and delete roles.</li><li>• View current group memberships and reassign roles.</li></ul> <p><a href="#">“Roles” on page 164</a> provides more information about roles.</p>
<b>Module Roles</b>	<p>Accesses the Modules Roles page. From the Modules Roles page you can</p> <ul style="list-style-type: none"><li>• Search for existing module roles.</li><li>• Create, modify, and delete module roles.</li><li>• View current group memberships and reassign module roles.</li></ul> <p><a href="#">“Module roles” on page 167</a> provides more information about module roles.</p>
<b>Sessions</b>	<p>Accesses the Sessions page. From the Sessions page you can</p> <ul style="list-style-type: none"><li>• Search for sessions.</li><li>• View session properties and session logs</li></ul> <p><a href="#">“Sessions” on page 170</a> provides more information about module roles.</p>

## 6.2 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 OpenText Documentum CM repository, user accounts are represented by user objects. Whenever a new user account is added to a repository, Documentum CM Server creates a user object. A user object specifies how a user can access a repository and what information the user can access.

## 6.2.1 Locating users

Use the search filters on the Users page to locate 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 “[User search filters](#)” on page 139.  
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 6-2: User search filters**

Field	Description
<b>User Name</b>	Filters the search results by user name.
<b>Default Group</b>	Filters the search results by the name of the default group.
<b>User Login Name</b>	Filters the search results by the login name of the user.
<b>User Login Domain</b>	Filters the search results by login domain.

## 6.2.2 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 "[User properties](#)" on page 140.
5. Click **OK**.

**Table 6-3: User properties**

Field	Description
<b>State</b>	Indicates the user account state in the repository. Valid values are: <ul style="list-style-type: none"><li>• <i>Active</i>: The user is a currently active repository user. Active users are able to connect to the repository.</li><li>• <i>Inactive</i>: The user is not currently active in the repository. Inactive users are unable to connect to the repository.</li><li>• <i>Locked</i>: The user is unable to connect to the repository.</li><li>• <i>Locked and inactive</i>: The user is inactive and unable to connect to the repository.</li></ul> If the user is a superuser, only another superuser can reset the state.
<b>Name</b>	The user name for the new user. The user name cannot be modified, but can be reassigned to another user. " <a href="#">Reassigning objects to another user</a> " on page 152 provides more information.
<b>User Login Name</b>	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.

<b>Field</b>	<b>Description</b>
<b>User Login Domain</b>	Identifies the domain in which the user is authenticated. This is typically a Windows domain used for authentication.
<b>User Source</b>	<p>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.</p> <ul style="list-style-type: none"> <li>• <i>None</i>: The user is authenticated in a Windows domain.</li> <li>• <i>UNIX only</i>: The user is authenticated using the default Linux mechanism, dm_check_password or other external password checking program.</li> <li>• <i>Domain only</i>: The user is authenticated against a Windows domain.</li> <li>• <i>UNIX first</i>: 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.</li> <li>• <i>Domain first</i>: 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.</li> <li>• <i>LDAP</i>: The user is authenticated through an LDAP directory server.</li> <li>• <i>OTDS</i>: The user is authenticated through OpenText Directory Services.</li> <li>• <i>Inline Password</i>: 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.</li> </ul>
<b>Password</b>	<p>The password for the user.</p> <p>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.</p> <p>This must be provided manually for users added using an imported LDIF file.</p>
<b>Confirm Password</b>	<p>The password for the user.</p> <p>This field is displayed if Inline Password is selected as the User Source. Enter the same password you entered in the <b>Password</b> field.</p>
<b>Description</b>	A description of the user account.
<b>E-Mail Address</b>	The email address of the user. This is the email address to which notifications are sent for workflow tasks and registered events.
<b>User OS Name</b>	The operating system user name of the user.

Field	Description
<b>Windows Domain</b>	The Windows domain associated with the user account or the domain on which the user is authenticated. The latter applies if Documentum CM Server is installed on a Linux host and Windows domain authentication is used.
<b>Home Repository</b>	The repository where the user receives notifications and tasks.
<b>User is global</b>	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.
<b>Restrict Folder Access To</b>	<p>Specifies which folders the user can access. Click <b>Select</b> 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.</p> <p>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.</p>
<b>Default Folder</b>	<p>The default storage place for any object the user creates. This option only displays when you are creating a user. Valid values are:</p> <ul style="list-style-type: none"> <li>• <i>Choose existing folder</i>: Select this option to assign a folder you already created as the default folder for that user.</li> <li>• <i>Choose/Create folder with the user name</i>: Select this option to automatically create a folder with the name of the user as the object name.</li> </ul>
<b>Default Group</b>	<p>The group that is associated with the default permission set of the user. Click <b>Select</b> to specify a default group.</p> <p>When the user creates an object in the repository, it automatically belongs to this group.</p>
<b>Default Permission Set</b>	The permission set that assigns the default permissions to objects the user creates. Click <b>Select</b> to specify a default permission set.
<b>Db Name</b>	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.

<b>Field</b>	<b>Description</b>
<b>Privileges</b>	<p>The privileges that are assigned to the user.</p> <p>User privileges authorize certain users to perform activities in the repository. Select one of the privileges from the drop-down list, as follows:</p> <ul style="list-style-type: none"> <li>• None</li> <li>• Create Type</li> <li>• Create Cabinet</li> <li>• Create Cabinet and Type</li> <li>• Create Group</li> <li>• Create Group and Type</li> <li>• Create Group and Cabinet</li> <li>• Create Group, Cabinet, and Type</li> <li>• System administrator</li> <li>• 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.</li> </ul>
<b>Extended Privileges</b>	<p>Specifies the auditing privileges for the user. Superusers and system administrators cannot modify their own extended privileges.</p> <ul style="list-style-type: none"> <li>• <i>None</i>: The user cannot configure auditing, view audit trails, or purge audit trails.</li> <li>• <i>Config audit</i>: The user can configure auditing.</li> <li>• <i>Purge audit</i>: The user can purge existing audit trails.</li> <li>• <i>Config and Purge Audit</i>: The user can configure auditing and purge existing audit trails.</li> <li>• <i>View Audit</i>: The user can view audit trails.</li> <li>• <i>Config and View Audit</i>: The user can configure auditing and view existing audit trails.</li> <li>• <i>View and Purge Audit</i>: The user can view existing audit trails and purge them.</li> <li>• <i>Config, View, and Purge Audit</i>: The user can configure auditing and view and purge existing audit trails.</li> </ul>

Field	Description
<b>Client Capability</b>	<p>Describes the expertise level of the user.</p> <p>The client capability setting is used by OpenText Documentum CM client products to determine which functionality to deliver to the user. Documentum CM Server does not recognize or use the client capability setting.</p> <p>Choose a user type from the list:</p> <ul style="list-style-type: none"><li>• Consumer</li><li>• Contributor</li><li>• Coordinator</li><li>• System Administrator</li></ul>
<b>Alias Set</b>	The default alias set for the user. Click <b>Select</b> to specify an alias set.
<b>Disable Workflow</b>	Indicates whether a user can receive workflow tasks.
<b>Disable Authentication Failure Checking</b>	If selected, user can exceed the number of failed logins specified in the Maximum Authentication Attempts field of the repository configuration object.

### 6.2.3 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](#)” on page 139 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.

## 6.2.4 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.

## 6.2.5 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.
4. Navigate to **Administration > User Management > Users**.
5. Select **File > Import Users**.  
The Import User page displays.
6. Enter the user information, as described in “[Import user properties](#)” [on page 147](#).
7. Click **Finish**.

**Table 6-4: Import user properties**

Field	Description
<b>State</b>	Indicates the user's state in the repository. Select one of the following: <ul style="list-style-type: none"><li>• <i>Active</i>: The user is a currently active repository user. Active users are able to connect to the repository.</li><li>• <i>Inactive</i>: The user is not currently active in the repository. Inactive users are unable to connect to the repository.</li></ul> If the user is a superuser, only another superuser can reset the state.
<b>Source</b>	The name of an input file. Click <b>Browse</b> to browse to the location of the LDIF file containing information for creating the new users.  <i>"Import file format" on page 150</i> provides more information about the LDIF file format.

Field	Description
<b>User Source</b>	<p>Specifies how to authenticate a given repository user's user name and password. Valid values are:</p> <ul style="list-style-type: none"> <li>• <i>None</i>: Windows only. This means the user is authenticated in a Windows domain.</li> <li>• <i>UNIX only</i>: The user is authenticated using the default Linux mechanism, <code>dm_check_password</code> or other external password checking program. This option only displays on Linux hosts.</li> <li>• <i>Domain only</i>: The user is authenticated against a Windows domain. This option only displays on Linux hosts.</li> <li>• <i>UNIX first</i>: This is used for Linux repositories where Windows domain authentication is in use. This option only displays on Linux hosts.</li> </ul> <p>The user is authenticated first by the default Linux mechanism. If the authentication fails, the user is authenticated against a Windows domain.</p> <ul style="list-style-type: none"> <li>• <i>Domain first</i>: This is used for Linux repositories where Windows domain authentication is in use. This option only displays on Linux hosts.</li> </ul> <p>The user is authenticated first against a Windows domain; if that fails, the user is authenticated by the default Linux mechanism.</p> <ul style="list-style-type: none"> <li>• <i>LDAP</i>: The user is authenticated through an LDAP directory server.</li> </ul>
<b>Description</b>	A description of the user account.
<b>E-Mail Address</b>	The email address of the user. This is the email address to which notifications are sent for workflow tasks and registered events.
<b>Windows Domain</b>	(Windows only) The domain name associated with the new user's Windows account.
<b>Home Repository</b>	The repository where the user receives notifications and tasks.
<b>User is global</b>	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.

Field	Description
<b>Default Folder</b>	The default storage place for any object the user creates. Click <b>Select</b> to assign a folder.
<b>Default Group</b>	<p>The group that is associated with the default permission set of the user. Click <b>Select</b> to specify a default group.</p> <p>When the user creates an object in the repository, it automatically belongs to this group.</p>
<b>Default ACL</b>	The permission set that assigns the default permissions to objects the user creates. Click <b>Select</b> to specify a default permission set.
<b>Db Name</b>	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.
<b>Privileges</b>	<p>The privileges that are assigned to the user.</p> <p>User privileges authorize certain users to perform activities in the repository. Select one of the privileges from the drop-down list, as follows:</p> <ul style="list-style-type: none"> <li>• None</li> <li>• Create Type</li> <li>• Create Cabinet</li> <li>• Create Cabinet and Type</li> <li>• Create Group</li> <li>• Create Group and Type</li> <li>• Create Group and Cabinet</li> <li>• Create Group, Cabinet, and Type</li> <li>• System Administrator</li> <li>• Superuser: If you grant superuser privileges to a user, add that user manually to the group called <code>admingroup</code>. If you revoke a user's superuser privileges, remove the user from the <code>admingroup</code>.</li> </ul>

Field	Description
<b>Client Capability</b>	Indicates what expertise level of the user. This option is for informative purposes only and is not associated with any privileges. Documentum CM Server does not recognize or enforce these settings.  Choose a user type from the list: <ul style="list-style-type: none"> <li>• Consumer</li> <li>• Contributor</li> <li>• Coordinator</li> <li>• System Administrator</li> </ul>
<b>Alias Set</b>	The default alias set for the user. Click <b>Select</b> to specify an alias set.
<b>If user exists, then overwrite user information</b>	Select this option if a user already exists in the repository and you want to replace existing information with the imported information.
<b>If user exists, then ignore information</b>	Select this option if a user already exists in the repository and you want to retain the existing information.

### 6.2.5.1 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 6-5: Default values for new users**

Argument	Default
user_login_name	username
privileges	0 (None)
folder	/username
group	docu
client_capability	1

Each *attribute\_name:attribute\_value* pair must be on a new line. For example:

```
object_type:dm_user
user_name:Pat Smith
user_group:accounting
acl_domain:smith
```

```
acl_name:Global User Default ACL
object_type:dm_user
user_name:John Brown
```

If the ldif file contains umlauts, accent marks, or other extended characters, store the file as a UTF-8 file, or users whose names contain the extended characters are not imported.

The attributes you can set through the LDIF file are:

```
user_name
user_os_name
user_os_domain
user_login_name
user_login_domain
user_password
user_address
user_db_name
user_group_name
user_privileges (set to integer value)
default_folder
user_db_name
description
acl_domain
acl_name
user_source (set to integer value)
home_docbase
user_state (set to integer value)
client_capability (set to integer value)
globally_managed (set to T or F)
alias_set_id (set to an object ID)
workflow_disabled (set to T or F)
user_xprivileges (set to integer value)
failed_auth_attempt (set to integer value)
```

You can specify as many of the 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.

Documentum CM Server creates the default folder for each user if it does not already exist.

### 6.2.6 Deleting users

You can remove users from the repository, but OpenText 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](#)” on page 152.

You can delete a user and then create a user with the same name. If you add a new user with the same name as a deleted user and have not removed references to the deleted user, the new user inherits the group membership and object permissions belonging to the deleted user.

You cannot delete the repository owner, installation owner, or yourself.

**To delete users:**

1. Navigate to **Administration > User Management > Users**.
2. Select the users to delete by checking the check boxes next to their names.
3. Select **File > Delete**.
4. Click **Finish**.

### 6.2.7 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**.

### 6.2.8 Changing the home repository of a user

The home repository is where users receive tasks and notifications in their inboxes.

#### To change a home repository:

1. Navigate to **Administration > User Management > Users**.
2. Select the user for whom you want to change the home repository.
3. Select **Tools > Change Home Repository**.
4. From the list, select the user's new home repository.
5. Indicate whether to run the job that changes the home repository when it is next scheduled or to run the job now.
6. Click **OK**.

### 6.2.9 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**.

### 6.2.10 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.

### 6.2.11 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.

### 6.2.12 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.

### 6.2.13 Reassign reports

This page displays reassign logs, including group and user reassign logs.

## 6.3 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](#)” on page 156 provides more information on dynamic groups.

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

**Table 6-6: Privileges for creating or modifying groups**

Privilege	Create	Modify	Delete
Create Group	Can create group or assign ownership to a group to which the user belongs.	Can add or delete members and assign ownership to a group to which the user belongs.	Can delete groups the user owns, including groups where a group is owner and the user is a member of the group.

Privilege	Create	Modify	Delete
System administrator	Can create group or assign ownership to a group to which the user belongs.	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.	Can delete groups the system administrator owns, including groups where a group is owner and the system administrator is a member of the group.
Superuser	Can create a group and assign ownership to a different user or group.	Can update group administrator, owner, or members of a group.	Can delete any group.

A group can own SysObjects and permission sets.

The name assigned to a group must consist of characters that are compatible with the Documentum CM 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.

### 6.3.1 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 Documentum CM 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 Documentum CM Server does not treat the user as a member of the group. The user cannot exercise the change ownership or change permissions permits through the group.

### 6.3.2 Privileged groups

Installing Documentum CM 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 6-7: Privileged groups**

Group	Description
dm_browse_all	Members of this group can browse any cabinets and folders in the repository, folders except the rooms that were created using Documentum Collaborative Services.  The dm_browse_all_dynamic is a member of this group by default.
dm_browse_all_dynamic	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.
dm_escalated_allow_save_on_lock	Used internally for RPS.  Created and managed by superusers only. Members of this group can modify and save changes to an object that is checked out by other users.

Group	Description
dm_retention_managers	<p>Members of this group can:</p> <ul style="list-style-type: none"> <li>Own retainer objects (representing retention policies)</li> <li>Add and remove a retainer from any SysObject.</li> <li>Add and remove content in a retained object</li> <li>Change the containment in a retained virtual document</li> </ul> <p>This is a non-dynamic group.</p>
dm_retention_users	<p>Members of this group can add retainers (retention policies) to SysObjects.</p> <p>This is a non-dynamic group.</p>
dm_superusers	<p>Members of this group are treated as superusers in the repository.</p> <p>The dm_superusers_dynamic group is a member of this group by default.</p>
dm_superusers_dynamic	<p>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.</p>
dm_sysadmin	<p>Members of this group are treated as users with system administrator user privileges.</p>
dm_create_user	<p>Member of this group have Create User user privilege.</p>
dm_create_type	<p>Member of this group have Create Type user privilege.</p>
dm_create_group	<p>Member of this group have Create Group user privilege.</p>
dm_create_cabinet	<p>Member of this group have Create Cabinet user privilege.</p>

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

- dm\_assume\_user
- dm\_datefield\_override
- dm\_escalated\_delete
- dm\_escalated\_full\_control
- dm\_escalated\_owner\_control

- dm\_escalated\_full\_control
- dm\_escalated\_relate
- dm\_escalated\_version
- dm\_escalated\_write
- dm\_internal\_attrib\_override
- dm\_user\_identity\_override

### 6.3.3 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.

### 6.3.4 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**.

### 6.3.5 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 “[Group properties](#)” on page 160.
  4. Click **OK** to save your changes.

**Table 6-8: Group properties**

Field	Description
<b>Name</b>	The name of the repository group.
<b>Group Native Room</b>	The group’s native room. This field appears only if the rooms feature of Collaborative Services is enabled.
<b>E-Mail Address</b>	The email address for the new group.  If no value is entered in this field, the group email address defaults to the group name.
<b>Owner</b>	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.
<b>Administrator</b>	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.
<b>Alias Set</b>	The default alias set for the group.
<b>Group is Global</b>	Displayed only in the governing repository of a federation and the group must be a global group.
<b>Description</b>	A description of the group.

<b>Field</b>	<b>Description</b>
<b>Private</b>	<p>Defines whether the group is private. If not selected, the group is created as a public group.</p> <p>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.</p> <p>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.</p> <p>A superuser can update any group, regardless if Private is enabled or not.</p>
<b>Dynamic</b>	<p>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.</p> <p><a href="#">“Dynamic groups” on page 156</a> provides more information on dynamic groups.</p>
<b>Protected</b>	<p>Indicates if the group is protected against adding or deleting members. Use of a protected dynamic group is limited to applications running with a Foundation Java API installation that has been configured as privileged through the Documentum Administrator client rights administration.</p> <p>The Protected check box is enabled only when Dynamic Group is selected.</p>

### 6.3.6 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**.

### 6.3.7 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)**.

### 6.3.8 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.

### 6.3.9 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**.

### 6.3.10 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**.

## 6.4 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.

### 6.4.1 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 “[Role properties](#)” on page 164.
4. Click **OK** to save your changes.

**Table 6-9: Role properties**

Field	Description
<b>Name</b>	The name of the repository role.
<b>Group Native Room</b>	The native room for the role. The field appears only if the rooms feature of Collaborative Services is enabled.
<b>E-Mail Address</b>	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.
<b>Owner</b>	The name of a repository user who has the Create Group privilege and who owns this role.
<b>Administrator</b>	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.
<b>Alias Set</b>	The default alias set for the role.

<b>Field</b>	<b>Description</b>
<b>Role Is Global</b>	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.
<b>Description</b>	A description of the role.
<b>Private</b>	<p>Defines whether the role is private. If not selected, the role is created as a public role.</p> <p>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.</p> <p>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.</p>
<b>Create role as domain</b>	<p>Select to create a dm_group object with group_class as domain.</p> <p>This field only appears on the New Role - Info page.</p>
<b>Dynamic</b>	<p>Indicates if the role a dynamic role. A dynamic role is a role whose list of members is considered a list of potential members. User membership is controlled on a session-by-session basis by the application at runtime. The members of a dynamic role comprise of the set of users who are allowed to use the role; but a session started by one of those users will behave as though it is not part of the role until it is specifically requested by the application.</p>
<b>Protected</b>	<p>Indicates if the role is protected against adding or deleting members. Use of a protected dynamic role is limited to applications running with a Foundation Java API installation that has been configured as privileged through the Documentum Administrator client rights administration.</p> <p>The Protected check box is enabled only when Dynamic Role is selected.</p>

## 6.4.2 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**.

## 6.4.3 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**.

#### 6.4.4 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 reassigned the members of the role to another role.

**To delete a role:**

1. Navigate to **Administration > User Management > Roles** to access the **Roles** list page.
2. Select the name of the role to delete.
3. Select **File > Delete**.
4. Click **OK**.

### 6.5 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.

#### 6.5.1 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 “[Module role properties](#)” on page 168.
  4. Click **OK** to save your changes.

**Table 6-10: Module role properties**

Field	Description
<b>Name</b>	The name of the repository module role.
<b>Group Native Room</b>	The native room for the module role. The field appears only if the rooms feature of Collaborative Services is enabled.
<b>E-Mail Address</b>	The email address for the module role.  If no value is entered in this field, the module role email address defaults to the module role name.
<b>Owner</b>	The name of a repository user who has the Create Group privilege and who owns this module role.
<b>Administrator</b>	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.
<b>Alias Set</b>	The default alias set for the module role.
<b>Module Role is Global</b>	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.
<b>Description</b>	A description of the module role.
<b>Private</b>	Defines whether the module role is private. If not selected, the module role is created as a public module role.  A module role with Private enabled can be updated only by a user who is the owner of the role or is listed as the roll administrator. A module role with Private not enabled can be updated by a user with system administrator privileges as well as by the role owner or administrator. A superuser can update any module role, regardless if Private is enabled or not.

Field	Description
<b>Protected</b>	Select to restrict the module role to be used only by applications running on a privileged client.

## 6.5.2 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**.

## 6.5.3 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**.

## 6.6 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, 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>>.

### 6.6.1 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. This is applicable only for superusers or the installation owner of Documentum CM Server.

#### 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.

This lists all the user sessions connected to a specific repository that they select in the Documentum Administrator user interface login page.

- To view user sessions, select **User Sessions** from the drop-down list.

This lists only the sessions of the current user connected to a specific repository that they select in the Documentum Administrator user interface login page.

## 6.6.2 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 6-11: Session information**

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

2. Click **OK** or **Cancel** to return to the Sessions page.

### 6.6.3 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.

### 6.6.4 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 7

## Security

### 7.1 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 “[Permissions Sets page](#)” on page 173

**Table 7-1: Permissions Sets page**

Field	Description
Name	The object name of the permission set.
Owner	The user or group that owns the permission set.
Class	Specifies set how the permission set is used: <ul style="list-style-type: none"><li>• <i>Regular</i>: The permission set can only be used by the owner.</li><li>• <i>Public</i>: The permission set can be used by any user.</li></ul>
Description	A description of the permission set.

#### 7.1.1 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.

## 7.1.2 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 “[Permission set properties](#)” on page 174.
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 “[Permission properties](#)” on page 175.
5. Click **OK** to save your changes.

Before the permission set is saved, Documentum CM Server validates the permission set, as described in “[Permission set validation](#)” on page 183.

**Table 7-2: Permission set properties**

Field	Description
<b>Name</b>	The name of the permission set.
<b>Description</b>	A description of the permission set.
<b>Owner</b>	Indicates who owns the permission set. <ul style="list-style-type: none"><li>• If connected as a superuser or the repository owner, you can change who owns the permission set.</li><li>• If creating a permission set and connected with user privileges other than superuser or the repository owner, you are the owner.</li></ul>
<b>Is Internal</b>	Specifies whether the permission set is implicitly created by the server (T) or explicitly created by the user (F).

Field	Description
<b>Class</b>	<p>Specifies the class for the permission set. Valid values are:</p> <ul style="list-style-type: none"> <li>• <b>Regular:</b> 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.</li> <li>• <b>Public:</b> 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.</li> </ul>
<b>Globally Managed</b>	<p>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.</p>

### 7.1.3 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 “[Permission properties](#)” on page 175.

**Table 7-3: Permission properties**

Field	Description
<b>Required Groups</b>	<p>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 Documentum CM Server allows access to the object.</p> <p>Click <b>Add</b> to access the Choose a group page to add groups to the permission set, of which a user must be a member of repositories.</p> <p>Select a group and click <b>Remove</b> to remove a required group.</p>

Field	Description
<b>Group</b>	Displays groups of which a user must be a member of repositories. If no groups are defined, the system displays the message <b>No Required Groups exist for the permission set.</b>
<b>Required Group Set</b>	<p>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.</p> <p>Click <b>Add</b> 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 repository.</p> <p>Select a group and click <b>Remove</b> to remove a group set.</p>
<b>Group</b>	Displays groups of which a user must be a member of at least one repository. If no groups are defined, the system displays the message <b>No Required Groups exist for the permission set.</b>
<b>Grant access to</b>	<p>The Documentum CM Server automatically adds dm_owner and dm_world to a permission set. The default alias dm_owner represents the owner of the permission set and dm_world represents all repository users. You cannot delete dm_owner or dm_world from a permission set.</p> <ul style="list-style-type: none"> <li>• Click <b>Add</b> to add users or groups and their permissions for the permission set.</li> <li>• Select a user and click <b>Edit</b> to modify basic or extended permissions.</li> <li>• Select a user and click <b>Remove</b> to delete a user or group from the permission set.</li> <li>• Select a user and click <b>Add to group</b> to add them to access the Add to Group page.</li> </ul>
<b>Accessors</b>	Displays users and groups who are included in the permission set.
<b>Permissions</b>	Displays the basic permission level access for the user or group. To change the basic permission level access, select a user and click <b>Edit</b> .
<b>Extended Permissions</b>	Displays the extended permissions for the user or group. To change the extended permissions, select a user and click <b>Edit</b> .

Field	Description
<b>Conflict</b>	<p>If there are validation conflicts, the system displays reasons for the conflicts. For example:</p> <ul style="list-style-type: none"> <li>• <b>Not a member of the following required group:</b> Indicates which required groups that a user currently does not have any membership to.</li> <li>• <b>Not a member of any required group set:</b> Indicates that the user currently is not a member of any group in the required group set.</li> </ul>
<b>Deny access to</b>	<p>An access restriction entry denies a user the right to the base object-level permission level specified in the entry. For example, if a user would otherwise have Delete permission as a member of a particular group, an access restriction might limit the user to, at most, Version permission. The user would therefore lose Write and Delete permissions.</p> <ul style="list-style-type: none"> <li>• Click <b>Add</b> to add users or groups to restrict their permissions for the permission set.</li> <li>• Select a user and click <b>Edit</b> to modify basic or extended permission restrictions.</li> <li>• Select a user and click <b>Remove</b> to delete an access restriction entry.</li> <li>• Select a user and click <b>Add to group</b> to access the Add to Group page to add the user to a group or group set.</li> </ul>
<b>Accessors</b>	Displays users and groups who have restricted permissions in the permission set.
<b>Denied Access Level</b>	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 <b>Edit</b> .
<b>Extended Restrictions</b>	Displays the extended restrictions for the user or group. To change the extended restrictions, select a user and click <b>Edit</b> .
<b>Conflict</b>	If there are validation conflicts, the system displays reasons for the conflicts.

### 7.1.4 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**.

### 7.1.5 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 check box next to the names of any users, groups, or roles to add to the permission set.

- b. Click the **Add** arrow.
  - c. Click **OK** or **Cancel**.
    - Click **OK** to add the users, groups, and roles to the permission set.  
The system displays the **Set Access Permission** page.
    - Click **Cancel** to cancel the operation and return to the Permissions page.
6. On the Set Access Permission page, select the basic and extended permissions for each user, group, or role being added.
  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.

## 7.1.6 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 check box 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.

### 7.1.7 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.
3. Select **File > Delete**.
4. Click **OK**.

### 7.1.8 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 check boxes.

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.

## 7.1.9 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.

### 7.1.10 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.
8. Click **OK** or **Cancel** on the Permissions page.



**Note:** The **OK** and **Cancel** buttons appear when only one check box is selected in the **Grant access to** section on the Permissions page. If more than one check box is selected, the **Previous**, **Next**, **Finish**, and **Cancel** buttons appear.

- 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.

### 7.1.11 Permission set validation

Documentum CM 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.

Documentum CM 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 8

## Audit management

### 8.1 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**.

### 8.2 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 “[Object auditing properties](#)” on page 186.

- 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 “[Object auditing properties](#)” on page 186.

- To remove an audit, select the object name and click **Unaudit**.

5. Click **OK** to save your changes.

**Table 8-1: Object auditing properties**

Field	Description
<b>Application Code</b>	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 <i>Internal</i> 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.
<b>Lifecycle</b>	Records objects that are attached to a lifecycle. Click <b>Select Lifecycle</b> to access the <b>Choose a lifecycle</b> page.  Select the correct lifecycle and then click <b>OK</b> .

Field	Description
<b>State</b>	Records only those objects attached to the lifecycle and in a particular state. Select a state from the drop-down list.
<b>Attributes</b>	Records the values of particular properties of the object in the audit trail. Click <b>Select Attributes</b> to access the <b>Choose an attribute</b> page.  Select the properties whose values you want to record, click <b>&gt;</b> , then click <b>Add</b> . To remove any properties, select them on the right-hand side of the page and click <b>&lt;</b> .  Click <b>OK</b> when you are finished.
<b>Has signature manifested</b>	Select to sign the audit trail.
<b>Include all subtypes</b>	Select to include all subtypes of the audited object type.
<b>Authentication required</b>	Select to require authentication for custom (user-defined) events that are audited.
<b>Add</b>	Click to access the <b>Choose an event</b> page and select the events you want to register.  Select one or more events to audit and click <b>&gt;</b> to move the events to the Selected Items column. To remove any events, select them in the Selected Items column and click <b>&lt;</b> . Click <b>OK</b> when you are finished.  To unregister any events, select them in the Event Name list and click <b>Remove</b> .

### 8.2.1 Choosing a type

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

## 8.3 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 8-2: Object instance auditing properties**

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

## 8.4 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 the right arrow icon 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**.

## 8.5 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 “Audit search properties” on page 191.
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 8-3: Audit search properties**

<b>Field</b>	<b>Description</b>
<b>Search By</b>	Indicates whether to use the criteria specified on the search page or a DQL query to search for the audit trail.  Do one of the following: <ul style="list-style-type: none"> <li>• Select the <b>Search criteria defined below</b> option and enter the search criteria.</li> <li>• Select the <b>DQL</b> option and enter a DQL query in the <b>Where Clause</b> field. Click <b>OK</b> to display the query results.</li> </ul>
<b>Events</b>	Restricts the search by events. Click <b>Select</b> and select one or more events and click <b>OK</b> .
<b>Object Name</b>	Restricts the search by object names. Select <b>Begins With</b> , <b>Contains</b> , or <b>Ends With</b> and type in a string.
<b>Versions</b>	Restricts the search by version. Type in a version.
<b>Look In</b>	Restricts the search to a particular folder. Click <b>Select Folder</b> and select the folder.
<b>Audit Dates</b>	Restricts the search by time. Click <b>Local Time</b> or <b>UTC</b> , then type or select a beginning date in the <b>From</b> field and an ending date for the search in the <b>Through</b> field.
<b>Type</b>	Restricts the search to a particular type. Click <b>Select Type</b> and select the type. To include subtypes of the type, click <b>Include Subtype</b> .
<b>Lifecycle</b>	Restricts the search to objects attached to a lifecycle. Click <b>Select Lifecycle</b> and select a lifecycle.
<b>Application Code</b>	Restricts the search to objects with an application code. Type the application code. To restrict the search to those audit trails that are signed, select <b>Has Signature</b> .
<b>Controlling Application</b>	Restricts the search to objects with a controlling application. Type the name of the application.

## 8.6 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, Documentum CM 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. The following table describes the information on the Audit Policies page.

**Table 8-4: Audit Policies page information**

Field	Description
Name	The name of the audit policy.
Accessor Name	The name of the user, group, or role that are assigned this audit policy.
Is Group	Indicates whether the user specified in the Accessor Name column is belongs to a group.

[“Creating, modifying, or deleting an audit policy” on page 192](#) provides information about creating or modifying an audit policy.

### 8.6.1 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 [“Audit policy information” on page 193](#).

- 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 “[Audit policy information](#)” on page 193.
  - 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 8-5: Audit policy information**

Field	Description
<b>Name</b>	The name of the audit policy.
<b>Accessor Name</b>	The user, group, or role to which this audit policy is assigned.
<b>Audit Policy Rules</b>	<p>Specifies the policy rules, as follows:</p> <ul style="list-style-type: none"> <li>Click <b>Add</b> to add a rule. The Create/Edit Rule page displays. Select an attribute and enter a value for the attribute.</li> <li>Select an attribute name, then click <b>Edit</b> to modify the rule. The Create/Edit Rule page displays. Modify the attribute.</li> <li>Select an attribute name, then click <b>Remove</b> to delete the rule. There must be at least one rule or condition to save the audit policy.</li> </ul>

## 8.6.2 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 8-6: Audit policy example values**

Field	Description
<b>Name</b>	Test
<b>Accessor Name</b>	user1
<b>Audit Policy Rules</b>	
<b>Attribute Name</b>	Attribute Value
<b>object_type</b>	type1
<b>is_archived</b>	T

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.

## 8.7 Registering audits

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

Select the properties as described in “[Object and object instance auditing properties](#)” on page 194 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 8-7: Object and object instance auditing properties**

Field	Description
<b>Attributes</b>	Records the values of particular properties of the object in the audit trail. Click <b>Select Attributes</b> to access the <b>Choose an attribute</b> page.  Select the properties whose values you want to record, click <b>&gt;</b> , then click <b>Add</b> . To remove any properties, select them on the right-hand side of the page and click <b>&lt;</b> .  Click <b>OK</b> when you are finished.

Field	Description
Add	<p>Click to access the <b>Choose an event</b> page and select the events you want to register.</p> <p>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 <b>OK</b> when you are finished.</p> <p>To unregister any events, select them in the Event Name list and click <b>Remove</b>.</p>

## 8.8 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**. Click **Remove** to remove an audit.

For object instance:

- To add or modify an audit, select the object, then click **Edit**. Click **Remove** to remove an audit.



**Note:** The **Add Audit** button is disabled for object instance.

## 8.9 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](#)” on page 190. 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.

# Chapter 9

## Job management

### 9.1 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 Documentum CM 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 (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.

*OpenText Documentum Content Management - Server and Server Extensions Installation Guide (EDCSY250400-IGD)* provides more information on federation and replication jobs.

## 9.1.1 Job descriptions

The jobs in the following sections are automatically created with each repository.

### 9.1.1.1 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. *OpenText Documentum Content Management - Server and Server Extensions Installation Guide (EDCSY250400-IGD)* provides complete information on replication and replication jobs.

### 9.1.1.2 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. *OpenText Documentum Content Management - Server and Server Extensions Installation Guide (EDCSY250400-IGD)* provides complete information on replication and replication jobs.

### 9.1.1.3 Asynchronous Write (dm\_AsyncronousWrite)

When users import documents in asynchronous mode, there may be instances where some or all content may not be immediately replicated from Branch Office Caching Services to Accelerated Content Services. This might happen if the Messaging Service server was not available or there were network issues between Branch Office Caching Services, Messaging Service, and/or Accelerated Content Services.

The Asynchronous Write job polls for content still in a parked state and generates new messages for the Messaging Service server to pass to Branch Office Caching Services 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 Messaging Service server. If a Branch Office Caching Services 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.

#### 9.1.1.4 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 9-1: dm\_AuditMgt arguments**

Argument	Description
window_interval	Defines window, in minutes, in which the job can run.
queueperson	Specifies the user who receives Inbox and email notifications from the job.
cutoff_days	Specifies the age of the objects to delete. The default value is 90 days.
custom_predicate	<p>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:</p> <ul style="list-style-type: none"> <li>• delete_flag=TRUE This condition cannot be modified.</li> <li>• dequeued_date=value (value is computed using the cutoff_days argument) This condition cannot be modified.</li> <li>• r_gen_source=1 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. You can also add other conditions (for example, event=approved) to the default custom predicate.</li> </ul>

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.

### 9.1.1.5 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 OpenText Global Technical Services 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 CM Server.

The Consistency Checker job is active by default and is set to run once a day.

### 9.1.1.6 Content replication (dm\_ContentReplication)

The Content Replication tool automates content replication between the component storage areas of a distributed storage area. A content replication job looks for all content not locally present, gets the files while connected to other sites, and performs an IMPORT\_REPLICA for each content file in need of replication. The job generates a report that lists each object replicated. The report is saved to the repository in /System/Sysadmin/Reports/ContentReplication.

If the report runs against the content at a remote distributed site, the report name will have the sites server configuration name appended. For example, if London is a remote site, its report would be found in /System/Sysadmin/Reports/ContentReplicationLondon.

In a distributed environment, the jobs argument values for the remote sites are based on those of the Content Replication job for the primary site, but the job name and target server will be unique for each site. The job name has the format:

`dm_ContentReplicationserverconfig.object_name`

The jobs target\_server property identifies the local server performing the replication using the format repository.serverconfig@hostname. The Content Replication job is inactive by default.

The Content Replication tool requires enough temporary disk space to transfer the largest content file to be replicated.

### 9.1.1.7 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 configuration 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.

### 9.1.1.8 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 Documentum CM Server and made available to client applications through the publishing operation.

### 9.1.1.9 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 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 configuration 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.

#### **9.1.1.10 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.

#### **9.1.1.11 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.

#### **9.1.1.12 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.

### 9.1.1.13 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.

### 9.1.1.14 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. *OpenText Documentum Content Management - Server and Server Extensions Installation Guide (EDCSY250400-IGD)* provides complete information on repository federations and the federation jobs.

### 9.1.1.15 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. *OpenText Documentum Content Management - Server and Server Extensions Installation Guide (EDCSY250400-IGD)* provides complete information on repository federations and the federation jobs.

### 9.1.1.16 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. *OpenText Documentum Content Management - Server and Server Extensions Installation Guide (EDCSY250400-IGD)* provides complete information on repository federations and the federation jobs.

### 9.1.1.17 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. *OpenText Documentum Content Management - Server and Server Extensions Installation Guide (EDCSY250400-IGD)* provides complete information on repository federations and the federation jobs.

### **9.1.1.18 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. *OpenText Documentum Content Management - Server and Server Extensions Installation Guide (EDCSY250400-IGD)* provides complete information on repository federations and the federation jobs.

### **9.1.1.19 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.

### **9.1.1.20 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.

#### 9.1.1.21 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. *iPlanet* documentation provides instructions for enabling the changelog feature.

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 configuration 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 configuration object.

### 9.1.1.22 Log purge (dm\_LogPurge)

The Log Purge tool deletes old logs. The logs and the locations from which they are deleted are:

**Table 9-2: Logs deleted by log purge job**

Log type	Delete from
Server log files	Documentum CM Server installation log location
Connection broker log files	Documentum CM Server installation log location
Agent Exec log files	Documentum CM Server installation log location
Session log files	Documentum CM Server installation log location
Result log files	Temp cabinet
Job log files	Temp cabinet
Job reports	/System/Sysadmim/Reports folder
Lifecycle log files	Documentum CM Server installation log location

Files are considered old and are deleted if they were modified prior to a user-defined cutoff date. By default, the cutoff date is 30 days prior to the current date. For instance, if you run Log Purge on July 27, all log files that were modified before June 28 are deleted. You can change the cutoff interval by setting the -cutoff\_days argument for the tool.

Log Purge generates a report that lists all directories searched and the files that were deleted. The report is saved in the repository in /System/Sysadmin/Reports/LogPurge.

The Log Purge tool is installed in the inactive state.

Site Caching Services logs are deleted by the SCS Log Purge job. “[SCS log purge \(dm\\_SCSLogPurgeJob\)](#)” on page 209 provides information on that job.

#### 9.1.1.23 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.

#### 9.1.1.24 Remove expired retention objects (dm\_RemoveExpiredRetnObjects)

The RemoveExpiredRetnObjects tool removes objects with expired retention dates from content-addressed storage areas. It is available only in repositories version 5.2.5 SP1 and later, and can be used only in content-addressable storage areas.

The tool invokes the CHECK\_RETENTION\_EXPIRED administration method to determine which objects to remove. By default, the tool operates only on objects stored in content-addressable storage areas that require a retention date. You can also direct the tool to operate on content-addressable storage areas that allow but do not require a retention date by setting the INCLUDE\_ZERO\_RETENTION\_OBJECTS argument. The tool never includes objects stored in content-addressable storage areas that do not allow retention periods. “[Storage](#)” on page 307 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 \(dm\\_DMclean\)](#)” on page 202 provides more information on Dmclean.

*OpenText Documentum Content Management - Server DQL Reference Guide (EDCCS250400-DRD)* provides more information about the method underlying `RemoveExpiredRetnObjects`.

#### **9.1.1.25 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.

### 9.1.1.26 SCS log purge (dm\_SCSLogPurgeJob)

Only repositories where you have installed Site Caching Services 5.2 or later 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.

### 9.1.1.27 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 configuration object.
- Version numbers of your server, RDBMS, and operating system.

The State of the Repository Report is installed in the active state.

### 9.1.1.28 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.

### 9.1.1.29 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.

### 9.1.1.30 Usage tracking (dm\_usageReport)

This job collates usage data from multiple global registries and can generate a variety of reports and documents about software usage.

Documentum CM Server tracks software usage by recording login times. The Documentum CM 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 Documentum CM 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](#)” on page 241. You can also generate a current report. To generate a current report, refer to “[Running jobs](#)” on page 240.

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.

### 9.1.1.31 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 group 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** 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” on page 153](#) provides more information about changing the home repository of user.

### 9.1.1.32 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” on page 152](#) provides more information about changing a user name.

#### **9.1.1.33 Version management (dm\_VersionMgt)**

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

*OpenText Documentum Content Management - Server Fundamentals Guide (EDCCS250400-GGD)* provides more information about the version.

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 \(dm\\_DMClean\)” on page 202](#).

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.

#### **9.1.1.34 WfmsTimer (dm\_WfmsTimer)**

The WfmsTimer tool checks running workflows for expired activity timers. OpenText Documentum Content Management (CM) Workflow Designer 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.

## 9.1.2 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](#)” on page 243 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, Branch Office Caching Services caching jobs, and job sequences. For instructions about creating a specific type of job, refer to:

- “[Creating replication jobs](#)” on page 220
- “[Creating records migration jobs](#)” on page 228
- “[Creating remove expired retention objects jobs](#)” on page 233
- “[Creating Branch Office Caching Services caching jobs](#)” on page 233
- “[Creating job sequences](#)” on page 236

**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 “[Job Info properties](#)” on page 213.
4. Click the **Schedule** tab and enter the job schedule information, as described in “[Job Schedule properties](#)” on page 215.
5. Click the **Method** tab and enter the job method information, as described in “[Job method properties](#)” on page 218.
6. Click the **SysObject Info** tab and enter the job SysObject information, as described in “[Creating, viewing, or modifying SysObject properties](#)” on page 219.
7. Click **Finish** to save your changes.

**Table 9-3: Job Info properties**

Field	Description
<b>Name</b>	The name of the job object.

Field	Description
<b>Job Type</b>	<p>A label identifying the job type.</p> <p>If you are creating a replication job, records migration job, remove expired retention object, Branch Office Caching Services caching job, or a job sequence, this field is automatically populated with the associated job type.</p>
<b>Trace Level</b>	<p>Controls how much information is recorded in trace logs. May be set from 0 to 10.</p> <p><a href="#">"Viewing job trace logs" on page 242</a> provides instructions on viewing trace logs.</p>
<b>Designated Server</b>	<p>When more than one server runs against a repository, use to designate a server to run the job. The default is <i>Any Running Server</i>.</p>
<b>State</b>	<p>Determines how the job runs:</p> <ul style="list-style-type: none"> <li>• If set to Active, the job runs as scheduled.</li> <li>• If set to Inactive, the job does not run automatically, but can be executed manually.</li> </ul>
<b>Job Start Date</b>	<p>Specifies when the job was started. This option is a read-only field that only displays for existing jobs.</p>
<b>Options</b>	
<b>Deactivate on Failure</b>	<p>Specifies whether to make the job inactive if it does not run successfully.</p>
<b>Run After Update</b>	<p>Specifies whether to run the job immediately after any changes to the job are saved.</p>
<b>Save If Invalid</b>	<p>Specifies whether to save the job object if Documentum Administrator is unable to validate the job.</p>
<b>Job Run History</b>	
<b>Last Run</b>	<p>Displays the last date and time the job ran and was completed. This option is a read-only field that displays for existing jobs.</p>
<b>Last Status</b>	<p>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.</p>
<b>Last Return Code</b>	<p>Displays the last value returned by the job. This option is a read-only field that displays for existing jobs.</p>

Field	Description
<b>Runs Completed</b>	Displays the number of times the job has run to completion. This option is a read-only field that displays for existing jobs.

### 9.1.3 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, Branch Office Caching Services 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.

 **Warning**

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 “[Job Schedule properties](#)” on page 215.
6. Click **OK**.

**Table 9-4: Job Schedule properties**

Field	Description
<b>Next Run Date and Time</b>	Specifies the next start date and time for the job. The default is the current date and time.
<b>Repeat</b>	Specifies the time interval in which the job is repeated.

Field	Description
<b>Frequency</b>	Specifies how many times the job is repeated. 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.
<b>End Date and Time</b>	Specifies the end date and time for the job. The default end date is 10 years from the current date and time.
<b>After</b>	Specifies the number of invocations after which the job becomes inactive.

#### 9.1.4 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.

**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**.

### 9.1.5 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 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 “[Job method properties](#)” on page 218.
3. Click **OK** to save the changes.

**Table 9-5: Job method properties**

Field	Description
<b>Method Name</b>	<p>Specifies the name of the method that is associated with the job.</p> <p>Click <b>Select Method</b> to display the <b>Choose a method</b> page. Select a method name and click <b>OK</b>.</p> <p>“<a href="#">Locating a method for a job</a>” on page 219 provides instructions to locate a method.</p>
<b>Arguments</b>	<p>Specifies the method arguments.</p> <p>Click <b>Edit</b> to display the <b>Method Arguments</b> page. Enter new arguments, remove unnecessary arguments, or change the values to the method by the job.</p> <p>Many jobs take the queueperson and window_interval arguments.</p> <ul style="list-style-type: none"> <li>• The queueperson argument defines which repository user receives the inbox and email notifications generated by the jobs. If you do not designate a repository user for a specific job, the notifications are sent to the user identified by the operator_name property of the server configuration object of the server. This property is set to the repository owner’s name by default.</li> <li>• The window_interval argument defines a window on either side of the job’s scheduled run time in which the job can run. This ensures that if a server must be restarted, the startup is not delayed by jobs that must be run.</li> </ul>
<b>Pass Standard Arguments</b>	<p>Select this option to pass the standard arguments for the method.</p> <p>The standard arguments are:</p> <ul style="list-style-type: none"> <li>• Repository owner</li> <li>• Repository name</li> <li>• Job ID</li> <li>• Trace level</li> </ul>

## 9.1.6 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**.

## 9.1.7 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 “[SysObject properties](#)” [on page 219](#).
3. Click **OK** to save your changes.

**Table 9-6: SysObject properties**

Field	Description
<b>Title</b>	A name or title for the object.
<b>Subject</b>	A subject that describes the object.
<b>Keywords</b>	One or more keywords that describe the object. Click <b>Edit</b> to add, modify, remove, or change the order of keywords.
<b>Authors</b>	One or more authors associated with the object. Click <b>Edit</b> to add, modify, remove, or change the order of authors.
<b>Owner Name</b>	The user who owns the object. Click <b>Edit</b> to add or modify the owner name.
<b>Version Label</b>	The version number of the object. Click <b>Edit</b> to add, modify, remove, or change the order of version numbers.

Field	Description
<b>Checkout Date</b>	The date on which the object was last checked out. This is a read-only property.
<b>Checked Out By</b>	The name of the user who checked out the object. This is a read-only property.
<b>Created</b>	The date on which the object was created. This is a read-only property.
<b>Creator Name</b>	The name of the user who created the object. This is a read-only property.
<b>Modified</b>	The date on which the object was last modified. This is a read-only property.
<b>Modified By</b>	The name of the user who modified the object. This is a read-only property.
<b>Accessed</b>	The date on which the object was last accessed. This is a read-only property.

### 9.1.8 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](#)” on page 236 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](#)” on page 226 provides complete information on choosing replication and security modes.

*OpenText Documentum Content Management - Server and Server Extensions Installation Guide (EDCSY250400-IGD)* provides more information about replication jobs.

**To create a replication job:**

1. Navigate to **Administration > Job Management > Jobs**.  
The **Jobs** list page displays.
2. Select **File > New > Replication Job**.  
The New Replication Job page displays with the Info tab selected.
3. Enter general replication job information on the **Info** tab, as described in “[Job Info properties](#)” on page 213.
4. Click the **Schedule** tab and enter schedule information for the replication job, as described in “[Job Schedule properties](#)” on page 215.
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](#)” on page 221.
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](#)” on page 222.
7. Click the **Replication Options** tab and enter replication job options for the replication job, as described in “[Setting replication job options](#)” on page 223.
8. Click the **SysObject Info** tab and enter SysObject information for the replication job, as described in “[Creating, viewing, or modifying SysObject properties](#)” on page 219.
9. Click **Finish** to save your changes.

### 9.1.8.1 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](#)” on page 220 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.

### 9.1.8.2 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” on page 220](#) 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.

### 9.1.8.3 Setting replication job options

The Replication Options tab displays when you are creating or modifying a replication job pages are used to set replication job options.

[“Creating replication jobs” on page 220](#) provides instructions on how to create new replication jobs.

**To set replication options:**

1. Enter the replication options, as described in [“Replication options” on page 223](#).
2. Click a tab to move to another Job Properties page, or click **OK** or **Cancel** to return to the Jobs list page.

**Table 9-7: Replication options**

Field	Description
<b>Code Page</b>	<p>Specifies the correct code page for the replication job. Keep the value at the default, UTF-8, unless it must be changed.</p> <p>Select <b>Full Refresh</b> 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.</p> <p>Select <b>Fast Replication</b>, to use fast replication.</p> <div style="text-align: center; margin-top: 10px;">  <b>Caution</b>            Fast replication does not replicate all relationships. <i>OpenText Documentum Content Management - Server and Server Extensions Installation Guide (EDCSY250400-IGD)</i> provides the detailed information.         </div>
<b>Full Text Indexing</b>	<p>Specifies the full-text indexing mode. Valid options are:</p> <ul style="list-style-type: none"> <li>• <b>Use target repository settings for indexing:</b> The same documents are indexed in the source and target.</li> <li>• <b>Do not index replicas:</b> None of the replicas are marked for indexing.</li> <li>• <b>Index all replicas:</b> All replicas in a format that can be indexed are marked for indexing.</li> </ul>

Field	Description
<b>Replication Mode</b>	<p>Specifies the replication mode.</p> <p>You can select federated mode whether or not the source and target repositories are in a federation. <a href="#">“Choosing replication and security modes” on page 226</a> provides more information on selecting a replication mode.</p> <p>Nonfederated replication mode is called as external replication mode in the <i>OpenText Documentum Content Management - Server and Server Extensions Installation Guide (EDCSY250400-IGD)</i>.</p>
<b>Security Option</b>	<p>Specifies how to handle security if there is no matching permission set in the target repository.</p> <ul style="list-style-type: none"> <li>• Select <b>Preserve</b> to replicate the source permission set in the target repository.</li> <li>• Select <b>Remap</b> 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.</li> </ul> <p><a href="#">“Choosing replication and security modes” on page 226</a> provides more information on choosing a security mode.</p>
<b>Maximum objects per transfer</b>	<p>Specifies the maximum number of objects dumped and transferred in each operation.</p> <p>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.</p> <p>Select <b>Manual Transfer</b> if you intend to manually move the dump file from the source to the target, then click <b>Select User</b> next to the <b>Transfer Operator</b> field.</p>

Field	Description
<b>Transfer operator</b>	<p>Specifies the user who manually transfers the replication job.</p> <p>Click <b>Select User</b> and select the user in the target repository to notify that a replication job is ready for manual transfer.</p> <p>The system sends an email notification to the selected user.</p> <div style="border: 1px solid #ccc; padding: 5px; margin-top: 10px;">  <b>Caution</b>            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.         </div>

#### 9.1.8.4 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**.

#### 9.1.8.5 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**.

#### **9.1.8.6 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**.

#### **9.1.8.7 Choosing a storage area**

On the Choose a storage page, select a storage area and then click **OK**.

#### **9.1.8.8 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 is called as external replication mode in the *OpenText Documentum Content Management - Server and Server Extensions Installation Guide (EDCSY250400-IGD)*. 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 “[Security mode behavior](#)” on page 227.

*OpenText Documentum Content Management - Server and Server Extensions Installation Guide (EDCSY250400-IGD)* provides more information about the two replication modes.

**Table 9-8: Security mode behavior**

<b>Selection</b>	<b>Replication Mode</b>
Federated and Preserve	<ul style="list-style-type: none"> <li>If the permission set of a replicated object exists in the target repository, the replica is assigned that permission set.</li> <li>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.</li> <li>Replica objects in the target repository are stored in the same storage area as in the source repository.</li> </ul> <p>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.</p>
Non-Federated and Preserve	<ul style="list-style-type: none"> <li>If the permission set of a replicated object exists in the target repository, the replica is assigned that permission set.</li> <li>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.</li> </ul> <p>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.</p> <ul style="list-style-type: none"> <li>Replica objects in the target repository are stored in the same storage area as in the source repository.</li> </ul> <p>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.</p>

Selection	Replication Mode
Federated and Remap	<ul style="list-style-type: none"> <li>• If the permission set of a replicated object exists in the target repository, the replica is assigned that permission set.</li> <li>• 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.</li> </ul> <p>This is the permission set selected on the Target tab. If no permission set is selected, 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.</p> <ul style="list-style-type: none"> <li>• Replica objects in the target repository are stored in the same storage area as in the source repository.</li> </ul> <p>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.</p>
Non-Federated and Remap	<ul style="list-style-type: none"> <li>• The replica is assigned the default replica permission set designated in the replication job.</li> </ul> <p>This is the permission set chosen on the Target tab. If no permission set is selected, 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.</p> <ul style="list-style-type: none"> <li>• Replica objects are stored in the replica storage area designated in the replication job.</li> </ul>

### 9.1.9 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.
2. Select **File > New > Records Migration Job**.  
The New Records Migration Job page displays with the **Info** tab selected.
3. Enter information on the **Info** tab, as described in “[Job Info properties](#)” on page 213.
4. Click the **Schedule** tab and enter schedule information for the records migration job, as described in “[Job Schedule properties](#)” on page 215.
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](#)” on page 229.
6. Click the SysObject Info tab and enter SysObject information for records migration job, as described in “[Creating, viewing, or modifying SysObject properties](#)” on page 219.
7. Click **Finish**.

### 9.1.9.1 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” on page 231* 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,1,object_name
myquery
setfile,c,1,C:\mig_query.txt,crtext
save,c,1
```
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” on page 232*.
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** check box when confident that the job runs as desired.

### 9.1.9.2 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** check box.
  - b. Select the **Use descend flag** check box 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** check box.
  - 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** check box.
  - b. Select the **Select attribute** link to access the **Choose an attribute** page, locate the correct property, select the check box 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** check box and type a version label.  
For example, type *CURRENT*.
5. To search all versions matching the selection criteria, select the **Search all versions** check box.
6. Click **OK**.

### 9.1.9.3 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**.

### 9.1.10 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 “[Job Info properties](#)” on page 213.
4. Click the **Schedule** tab and enter schedule information for the remove retention expired objects job, as described in “[Job Schedule properties](#)” on page 215.
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](#)” on page 216.
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](#)” on page 219.
7. Click **Finish**.



**Note:** “[Remove expired retention objects \(dm\\_RemoveExpiredRetnObjects\)](#)” on page 207 contains information to remove expired retention objects tool.

### 9.1.11 Creating Branch Office Caching Services caching jobs

A Branch Office Caching Services 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 Branch Office Caching Services destination information where the documents need to be.
- Sends caching requests to Messaging Service on a predetermined schedule.

Any user type can create a Branch Office Caching Services caching job. DQL queries for Branch Office Caching Services caching jobs are not validated.

#### To create a Branch Office Caching Services caching job:

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

2. Select **File > New > BOCS Caching Job**.
3. On the **Info** tab, type the basic information for the Branch Office Caching Services caching job on the Info tab, as described in “[Job Info properties](#)” on page 213.
4. Click the **Schedule** tab and enter schedule information for the Branch Office Caching Services caching job, as described in “[Job Schedule properties](#)” on page 215.
5. Click the Caching Rules tab and enter caching information for the Branch Office Caching Services caching job, as described in “[Caching rules properties](#)” on page 234.
6. Click the SysObject Info tab and enter Sysobject information for the Branch Office Caching Services caching job, as described in “[Creating, viewing, or modifying SysObject properties](#)” on page 219.
7. Click **Finish** to save your changes.

#### 9.1.11.1 Setting Branch Office Caching Services caching rules

The caching rules specify the caching options and the content to be selected for caching to the Branch Office Caching Services servers.

“[Creating Branch Office Caching Services caching jobs](#)” on page 233 provides complete instructions on how to create a Branch Office Caching Services caching job.

**Table 9-9: Caching rules properties**

Field	Description
Object Type	<p>The type of objects needed to create caching messages. By default, dm_sysobject is selected.</p> <p>Click <b>Select</b> to access the Choose a type page to select an object type.</p>

Field	Description
<b>Selection Criteria</b>	<p>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.</p> <ul style="list-style-type: none"> <li>• Select <b>Build criteria (Maximum of 5 lines)</b> to create up to five lines using query builder. The first query section will have the property name; the second query section will have the condition (operator); the third query section will hold the value (operand).</li> <li>• Select <b>DQL query</b> to create more complex queries. There are no restrictions on the number of conditions in a DQL query. DQL queries for Branch Office Caching Services caching jobs are not validated.</li> </ul>
<b>Network Location</b>	<p>The destination list of the cached content. Click <b>Select</b> to access the Choose Network Locations page to select from which network locations the content should be cached.</p>
<b>Cutoff Date</b>	<p>Select a cutoff date preference. The caching method compares the cutoff date to the last updated date of the document to determine if a caching request needs to be generated for the document.</p> <ul style="list-style-type: none"> <li>• Select <b>Cache all selected content</b> to cache all documents without considering the last modified date of the document.</li> <li>• Select <b>Cache only selected content added/modified after</b> and then select a date, hour, minute, and second to cache documents based on the selected date and time criteria.</li> </ul>
<b>Expiration</b>	<p>Enter an expiration date at which the caching request will expire if it is not fulfilled by that date.</p>
<b>Previous</b>	<p>Click to move to the previous page.</p>
<b>Next</b>	<p>Click to move to the next page.</p>
<b>OK or Finish</b>	<p>Click to save the changes and return to the Jobs list page.</p>
<b>Cancel</b>	<p>Click to return to the Jobs list page without saving any changes.</p>

### 9.1.12 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 “[Job Info properties](#)” on page 213.

4. Click the **Schedule** tab and enter the job schedule information, as described in “[Job Schedule properties](#)” on page 215.
5. Click the **Connection Info** tab and enter the repository and job sequence information, as described in “[Job Connection Info properties](#)” on page 237.
6. Click the **SysObject Info** tab and enter the job SysObject information, as described in “[Creating, viewing, or modifying SysObject properties](#)” on page 219.
7. Click **Finish**.

The job is saved and the Jobs list page appears.

#### **9.1.12.1 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 “[Job Connection Info properties](#)” on page 237.
2. Click **Finish**.

**Table 9-10: Job Connection Info properties**

Field	Description
<b>Job Repositories</b>	
<b>Add</b>	<p>Click <b>Add</b> to access the Choose Repositories page.</p> <p>The system displays a list of available repositories. Select the repositories in which you want to run jobs, click <b>Add</b>, then click <b>OK</b>.</p> <p>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</a>” on page 61 provides more information about adding a connection broker.</p>
<b>Remove</b>	To remove a repository from the list, select the repository and click <b>Remove</b> . If jobs in the repository are part of the sequence, you must remove the jobs first.

Field	Description
<b>Repository</b>	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.
<b>User Name</b>	The login name for the repository.
<b>Password</b>	The password for the repository.
<b>Domain</b>	Specify the domain for any repository running in domain-required mode.
<b>Job Sequence Information</b>	
<b>Add</b>	<p>Click <b>Add</b> 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 <b>Add</b>, then <b>OK</b>.</p> <p>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.</p>
<b>Job Name</b>	The name of the job that are in the job sequence.
<b>Job Dependencies</b>	<p>Specifies the dependencies the job has on other jobs.</p> <p>Click <b>Edit</b> 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 <b>OK</b>. 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.</p> <p>To remove a dependency, click <b>Edit</b> in the Job Sequence section to access the Choose jobs dependency page, clear the check box for any selected job, then click <b>OK</b>.</p>
<b>Repository</b>	The name of the repository where the job sequence is run.

### 9.1.12.2 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**.

### 9.1.12.3 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.

### 9.1.13 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](#)” on page 215 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.

### 9.1.14 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**.

### 9.1.15 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.

### 9.1.16 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.

### 9.1.17 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](#)” on page 241 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.

### 9.1.18 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.

### 9.1.19 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** check box.
4. Click **OK**.

## 9.2 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](#)” on page 197 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 \$DM\_JMS\_HOME/webapps/DmMethods/WEB-INF/lib directory. For workflow methods, the .jar files must be placed under the Process Engine deployment in the \$DM\_JMS\_HOME/webapps/bpm/WEB-INF/lib directory.

By default, all repositories contain methods used by Documentum CM Server. All methods with object names that begin with dm\_ are default methods.

## 9.2.1 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 Documentum CM 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 Documentum CM 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](#)” on page 250.

3. Enter or modify the method information as described in “[Method Info tab properties](#)” on page 245 and the optional “[SysObject Info tab properties](#)” on page 247.

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](#)” on page 248.

**Table 9-11: Method Info tab properties**

<b>Field</b>	<b>Description</b>
<b>Name</b>	The method name.  Do not use the format dm_<methodname> to name the method. This naming convention is reserved for default OpenText Documentum CM objects.
<b>Verb</b>	The method verb, including arguments.  The method verb is the command-line name of the procedure or the name of the interpretive language that executes the program file.  You can specify a full path, a relative path, or no path for the method verb. If you do not specify a path, the server searches the directories in the search path of the user.  To store the program as the content of the method object, you must import the content after you created the method, as described in <a href="#">"Importing method content" on page 248</a> .
<b>Method Type</b>	Specifies the programming language of the method. Valid values are: <ul style="list-style-type: none"> <li>• <i>dmbasic</i>: The method is written in Docbasic.</li> <li>• <i>dmawk</i>: The method is written in dmawk.</li> <li>• <i>java</i>: The method is written in Java and executed on the Java Method Server.</li> <li>• <i>program</i>: The method is writing in a programming language, such as C or C++.</li> </ul> If the method is executed using Documentum CM 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 pass all arguments specified on the DO_METHOD command line to the program.
<b>Arguments</b>	Specifies method arguments. Click <b>Edit</b> to add arguments.
<b>Method Success Codes</b>	Specifies method success codes. Click <b>Edit</b> to add success codes.

Field	Description
<b>Method Success Status</b>	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.
<b>Timeout Minimum</b>	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.
<b>Timeout Default</b>	<p>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.</p> <p>The default timeout value is 60 seconds and cannot be greater than the value specified in the timeout maximum field.</p>
<b>Timeout Maximum</b>	The maximum timeout that can be specified on the command line for this procedure. The default is 300 seconds.
<b>Launch Direct</b>	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.
<b>Launch Asynchronously</b>	<p>Specifies whether the server runs the method asynchronously or not.</p> <p>If this option is selected and the method is launched on the application server, setting <b>SAVE_RESPONSE</b> on to TRUE on the command line is ignored.</p> <p>If this option is select and the method is launched on the method server or Documentum CM Server and <b>SAVE_RESULTS</b> is set to TRUE on the command line, the method is always launched synchronously.</p>

Field	Description
<b>Run As Owner</b>	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.  This option must be selected to execute a method on the method server or application server.
<b>Trace Launch</b>	Specifies whether to save internal trace messages generated by the method to the session log.
<b>Use Method Server</b>	Specifies whether to use the dmbasic method server or Java method server to execute a dmbasic or Java method.
<b>Restartable</b>	Specifies whether the method can be restarted, if the Java Method Server crashes or fails to respond.  This option is only available for non-system Java methods.
<b>Failover Awareness</b>	Specifies whether the method is enabled for failover, if the server is associated with more than one Java Method Server.  This option can only be configured for non-system Java methods.

**Table 9-12: SysObject Info tab properties**

Field	Description
<b>Title</b>	A descriptive title for the method.
<b>Subject</b>	A subject associated with the method.
<b>Keywords</b>	One or more keywords that describe the method. Click <b>Edit</b> to add keywords.
<b>Authors</b>	One or more method authors. Click <b>Edit</b> to add authors.
<b>Owner Name</b>	The name of the method owner. Click <b>Edit</b> to select a different owner.
<b>Version Label</b>	The current version label of the method. Click <b>Edit</b> to change the version label.
<b>Checkout Date</b>	The date when the method was checked out last.
<b>Checked Out by</b>	The name of the user who checked out the method.

Field	Description
<b>Created</b>	The date and time when the method was created.
<b>Creator Name</b>	The name of the user who created the method.
<b>Modified</b>	The date and time when the method was last modified.
<b>Modified By</b>	The name of the user who last modified the method.
<b>Accessed</b>	The time and date when the method was last accessed.

## 9.2.2 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](#)” on page 244 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.

## 9.2.3 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 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 method from this page, select the check box unless you are logged in as the installation owner. The check box 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.

### 9.2.4 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.

### 9.2.5 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.

### 9.2.6 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** check box.
7. Click **OK**.
- The file is checked in.

### 9.2.7 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** check box 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.

### 9.2.8 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.

## 9.3 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.

### 9.3.1 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.

### 9.3.2 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**.

Content methods:

- CAN\_FETCH
- CLEAN\_LINKS
- DELETE\_REPLICA
- DESTROY\_CONTENT
- EXPORT\_TICKET\_KEY
- GET\_PATH
- IMPORT\_REPLICA
- IMPORT\_TICKET\_KEY
- MIGRATE\_CONTENT
- PURGE\_CONTENT
- REPLICATE
- RESTORE\_CONTENT
- SET\_STORAGE\_STATE

Database methods:

- DB\_STATS
- DROP\_INDEX
- EXEC\_SQL
- FINISH\_INDEX\_MOVES
- GENERATE\_PARTITION\_SCHEME\_SQL
- MAKE\_INDEX

- MOVE\_INDEX

Full-text indexing methods:

- ESTIMATE\_SEARCH
- MARK\_FOR\_RETRY
- MODIFY\_TRACE

Trace methods:

- GET\_LAST\_SQL
- MODIFY\_TRACE
- LIST\_RESOURCES
- LIST\_TARGETS
- SET\_OPTIONS

Workflow methods:

- RECOVER\_AUTO\_TASKS
- WORKFLOW\_AGENT\_MANAGEMENT

### 9.3.2.1 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 check boxes next to the objects whose content object IDs you want and click **Add**.
  - f. To remove an object from the list, select the check box 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.

### 9.3.2.2 **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** check box.  
The default is to clean only inactive sessions.
4. Click **Run**.  
The results are displayed.
5. Click **Close**.  
The Administration Methods page is displayed.

### 9.3.2.3 **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 check boxes next to the objects whose content object IDs you want and click **Add**.
  - f. To remove an object from the list, select the check box 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.

#### 9.3.2.4 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.

#### 9.3.2.5 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.

### 9.3.2.6 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 check boxes next to the objects whose content object IDs you want and click **Add**.
  - f. To remove an object from the list, select the check box 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.

### 9.3.2.7 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 check boxes next to the objects whose content object IDs you want and click **Add**.
  - f. To remove an object from the list, select the check box 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.

### 9.3.2.8 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 Documentum CM Server after successfully importing the login ticket to make your changes take effect.

### 9.3.2.9 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 “[Parameters for moving a single object](#)” on page 261.
4. Click **Run**.

**Table 9-13: Parameters for moving a single object**

Field	Description
<b>Migrate</b>	Select <b>A single object</b> from the drop-down list.

Field	Description
<b>Content</b>	<p>Click <b>Select Object</b>, then select an object type from the <b>Select From</b> drop-down list.</p> <p>Specify a limiting Where clause, or leave the <b>Where</b> field blank to select from all objects in the repository. To display all object versions, select the <b>Use all versions</b> check box and then click <b>Go</b>.</p> <p>Select <b>Remove the original source</b> to remove the original content file. The <b>Remove the original source</b> option cannot be edited, if the selected object belongs to an external store.</p> <p>Select the objects to migrate and click <b>Add</b>.</p>
<b>Path</b>	Click <b>Select Path</b> and select a location on the server file system for the log file path.
<b>Target</b>	Select a target file store from the drop-down list.
<b>Source Direct Access</b>	<p>Specifies whether the content files in the source store can be directly accessed through a full file path.</p> <p>This option is only available if the <b>Source</b> is an external store other than OpenText™ Documentum™ Content Management XML Store and the <b>Target</b> is either a file store or a ca store.</p>
<b>Migrate With</b>	<p>Specifies whether the source content is copied or moved to the target store during migration. Direct Move is applicable to file stores only.</p> <p>This option is only available if the <b>Source</b> is an external store and the <b>Target</b> is either a file store or a ca store.</p>
<b>Update Only</b>	<p>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 <b>Command File Name</b> field.</p> <p>This option is only available if the <b>Source</b> is an external store and the <b>Target</b> is either a file store or a ca store.</p>

Field	Description
<b>Command File Name</b>	A string that specifies a file path to a log file.  This option is only available if the <b>Source</b> is an external store and the <b>Target</b> is either a file store or a ca store and if the <b>Update Only</b> option is selected.

**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 “[Parameters for moving all content in a store](#)” on page 263.
4. Click **Run**.

**Table 9-14: Parameters for moving all content in a store**

Field	Description
<b>Migrate</b>	Select <b>All content in a filestore</b> from the drop-down list.
<b>Source</b>	Select a source file store from the <b>Source</b> drop-down list.  Select <b>Remove the original source</b> to remove the original content file. The <b>Remove the original source</b> option cannot be edited, if the selected object belongs to an external store.
<b>Path</b>	Click <b>Select Path</b> and select a location on the server file system for the log file path
<b>Target</b>	Select a target file store from the drop-down list.
<b>Maximum</b>	Specifies the maximum number of objects to migrate.  The default is to migrate all objects.
<b>Batch Size</b>	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.

Field	Description
<b>Content Migration Threads</b>	<p>Specifies the number of internal sessions used to execute the method.</p> <p>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.</p> <p>This option requires Content Storage Services on Documentum CM Server.</p>
<b>Source Direct Access</b>	<p>Specifies whether the content files in the source store can be directly accessed through a full file path.</p> <p>This option is only available if the <b>Source</b> is an external store other than OpenText Documentum Content Management (CM) XML Store and the <b>Target</b> is either a file store or a ca store.</p>
<b>Migrate With</b>	<p>Specifies whether the source content is copied or moved to the target store during migration. Direct Move is applicable to file stores only.</p> <p>This option is only available if the <b>Source</b> is an external store and the <b>Target</b> is either a file store or a ca store.</p>
<b>Update Only</b>	<p>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 <b>Command File Name</b> field.</p> <p>This option is only available if the <b>Source</b> is an external store and the <b>Target</b> is either a file store or a ca store.</p>
<b>Command File Name</b>	<p>A string that specifies a file path to a log file.</p> <p>This option is only available if the <b>Source</b> is an external store and the <b>Target</b> is either a file store or a ca store and if the <b>Update Only</b> option is selected.</p>

#### 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 “[Parameters for moving content selected by a query](#)” on page 265.
4. Click **Run**.

**Table 9-15: Parameters for moving content selected by a query**

Field	Description
<b>Migrate</b>	Select All content satisfying a query from the drop-down list.
<b>Select Object Type to Migrate</b>	Specify the object type to migrate.  If you select <b>dm_sysobject or it's subtype</b> , click <b>Select</b> to access the Choose a type page to select a subtype of <b>dm_sysobject</b> .
<b>Select r_object_id from dmr_content where</b>	Specify the DQL query.  Select <b>Remove the original source</b> to remove the original content file. The <b>Remove the original source</b> option cannot be edited, if the selected object belongs to an external store.
<b>Path</b>	Click <b>Select Path</b> and select a location on the server file system for the log file path
<b>Target</b>	Select a target file store from the drop-down list.
<b>Maximum</b>	Specifies the maximum number of objects to migrate.  The default is to migrate all objects.
<b>Batch Size</b>	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.
<b>Content Migration Threads</b>	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.  This option requires Content Storage Services on Documentum CM Server.

Field	Description
<b>Source Direct Access</b>	<p>Specifies whether the content files in the source store can be directly accessed through a full file path.</p> <p>This option is only available if the <b>Source</b> is an external store other than XML Store and the <b>Target</b> is either a file store or a ca store.</p> <p>Ensure that the <b>Source Direct Access</b> option is not selected if the query is run on objects stored in XML Stores.</p>
<b>Migrate With</b>	<p>Specifies whether the source content is copied or moved to the target store during migration. Direct Move is applicable to file stores only.</p> <p>This option is only available if the <b>Source</b> is an external store and the <b>Target</b> is either a file store or a ca store.</p>
<b>Update Only</b>	<p>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 <b>Command File Name</b> field.</p> <p>This option is only available if the <b>Source</b> is an external store and the <b>Target</b> is either a file store or a ca store.</p>
<b>Command File Name</b>	<p>A string that specifies a file path to a log file.</p> <p>This option is only available if the <b>Source</b> is an external store and the <b>Target</b> is either a file store or a ca store and if the <b>Update Only</b> option is selected.</p>

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 \(dm\\_DMfilescan\)](#)” on page 203.

### 9.3.2.10 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 check boxes next to the objects whose content object IDs you want and click **Add**.
  - e. To remove an object from the list, select the check box 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.

### 9.3.2.11 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.

### 9.3.2.12 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 Documentum CM 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 check box next to the object whose content object IDs you want and click **Add**.
  - e. To remove an object from the list, select the check box 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 check box 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.

### 9.3.2.13 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.

### 9.3.2.14 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.

### 9.3.2.15 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.

### 9.3.2.16 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.

### 9.3.2.17 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.

### 9.3.2.18 GENERATE\_PARTITION\_SCHEME\_SQL

The GENERATE\_PARTITION\_SCHEME\_SQL administration method is available to administrators and superusers. These additional restrictions apply:

- The method is available only on version 6.5 repositories.

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 OpenText Documentum CM 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 [“GENERATE\\_PARTITION\\_SCHEME\\_SQL parameters” on page 275](#).

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 9-16: GENERATE\_PARTITION\_SCHEME\_SQL parameters**

Parameter	Description
Operation	<p>Select an operation from the dropdown list box to define the subcommand. The options are:</p> <ul style="list-style-type: none"> <li>• <i>DB_PARTITION</i>: Generates a script to upgrade or convert a repository to a 6.5 partitioned repository. If selected: <ul style="list-style-type: none"> <li>– Select Partition Type or Table Name.</li> <li>– If Table Name is defined, optionally define the Owner Name.</li> <li>– Include object type is optional. Select to apply the partition operation to the dmi_object_type table.</li> <li>– Last Partition and Last Tablespace are optional.</li> <li>– In the Partitions section, Partition Name, Range, and Tablespace are required.</li> </ul> </li> <li>• <i>ADD_PARTITION</i>: Generates a script to add a partition to a partitioned type. If selected: <ul style="list-style-type: none"> <li>– Select Partition Type or Table Name.</li> <li>– If Table Name is defined, optionally define the Owner Name.</li> <li>– Include object type is optional. Select to apply the partition operation to the dmi_object_type table.</li> <li>– In the Partitions section, Partition Name, Range, and Tablespace are required.</li> </ul> </li> <li>• <i>EXCHANGE_PARTITION</i>: Generates a script for bulk ingestion by loading data from an intermediate table into a new partition of a partitioned table. If selected: <ul style="list-style-type: none"> <li>– Partition Type and Table Name are mutually exclusive.</li> <li>– If Table Name is defined, optionally define the Owner Name.</li> <li>– Include object type is optional. Select to apply the partition operation to the dmi_object_type table.</li> <li>– Partition Name, Range, and Tablespace are required.</li> <li>– Temp Table Suffix is optional.</li> </ul> </li> </ul>

Parameter	Description
Partition Type	Select a partition type from the dropdown list box, which displays a list of the partition types available for the repository. <i>All</i> 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.
Partition Name	Type a name for the partition. For DB_PARTITION and ADD_PARTITION operations, you must first click <b>Add</b> in the <b>Partitions</b> section to add information for each partition.
Range	Type the upper limit for the partition key range. For DB_PARTITION and ADD_PARTITION operations, you must first click <b>Add</b> in the <b>Partitions</b> section to add information for each partition.
Tablespace	Type the partition tablespace name. If not specified, the default tablespace is used. For DB_PARTITION and ADD_PARTITION operations, you must first click <b>Add</b> in the <b>Partitions</b> section to add information for each partition.
Temp Table Suffix	Type a temporary table suffix. This field is enabled and optional only if EXCHANGE_PARTITION is selected as the operation.

### 9.3.2.19 **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.

### **9.3.2.20 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.

### **9.3.2.21 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.

**9.3.2.22 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). *OpenText Documentum Content Management - Server DQL Reference Guide (EDCCS250400-DRD)* provides more information.

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.

### 9.3.2.23 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 Documentum CM 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.

### 9.3.2.24 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.

### 9.3.2.25 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:

Parameter	Description
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.

Parameter	Description
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.

### 9.3.2.26 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 configuration 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.

### 9.3.2.27 SET\_OPTIONS

The SET\_OPTIONS administration method turns tracing options on or off. You can set the following options:

Option	Action
clean	Removes the files from the server common area.
crypto_trace	Cryptography information.
debug	Traces session shutdown, change check, launch and fork information.
docbroker_trace	Traces connection broker information.
i18n_trace	Traces client session locale and codepage. An entry is logged identifying the session locale and client code page whenever a session is started.  An entry is also logged if the locale or code page is changed during the session.

Option	Action
last_sql_trace	<p>Traces the SQL translation of the last DQL statement issued before access violation and exception errors.</p> <p>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.</p> <p>It is strongly recommended that you do not turn off this option. It provides valuable information to OpenText Global Technical Services if it ever necessary to contact them.</p>
lock_trace	Traces Windows locking information.
net_ip_addr	Traces the IP addresses of client and server for authentication.
nettrace	Turns on RPC tracing. Traces Netwise calls, SSL, connection ID, client host address, and client host name.
sql_trace	SQL commands sent to the underlying RDBMS for subsequent sessions, including the repository session ID and the database connection ID for each SQL statement.
trace_authentication	Traces detailed authentication information.
trace_complete_launch	Traces Linux process launch information.
trace_method_server	Traces the operations of the method server.

The SET\_OPTIONS method returns TRUE if the operation succeeds or FALSE if it fails.

You must have 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 check box.
5. Click **Run**.  
The method runs and the results are displayed.

6. Click **Close**.

The system displays the Administration Methods list page.

### 9.3.2.28 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 Documentum CM Server.

If a Documentum CM 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 Documentum CM 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 Documentum CM 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.

### 9.3.2.29 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. Documentum CM 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: Documentum CM Server waits for the specified time for the workflow agent to shut down gracefully. If the time is exceeded, Documentum CM Server shuts down the workflow agent.
- 0: Documentum CM Server shuts down the workflow agent immediately.

If you do not provide a timeout value, Documentum CM Server uses the timeout value specified in the System Shutdown Timeout property of the server configuration 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 Documentum CM Server containing the workflow agent is down.
- The Documentum CM 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*.

### **9.3.2.30 Administration Methods Results Page**

This page displays the results of running an administration method.

### **9.3.2.31 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 10

# Alias sets and aliases

## 10.1 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. Documentum CM 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.

## 10.2 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 “[Alias set properties](#)” on page 290.
4. Click **Next** or select the **Aliases** tab.
5. Add aliases to the alias set.
6. Click **Finish**.

**Table 10-1: Alias set properties**

Field	Description
<b>Name</b>	The name of the alias set.
<b>Description</b>	A description of the alias set.
<b>Owner</b>	The name of the alias set owner. Click <b>Select</b> to select and assign an owner to the alias set.

## 10.3 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.

Property	Description
<b>Name</b>	The name of the alias.
<b>Category</b>	The category to which the alias belongs.
<b>Value</b>	The value assigned to the alias.
<b>Description</b>	A description of the alias.

4. To remove an alias from the alias set, select the alias and click **Remove**.
5. Click **OK** to save your changes.

## 10.4 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 [“Alias properties” on page 291](#).
6. Click **OK** to save alias additions, modifications, or deletions and return to the Alias Sets list page.

**Table 10-2: Alias properties**

Field	Description
Name	The name of the alias.  For an existing alias, the name is a read-only value and cannot be modified.

Field	Description
<b>Category</b>	<p>The category to which the alias belongs. The category can have the following values:</p> <ul style="list-style-type: none"> <li>• Permission Set</li> <li>• Cabinet Path</li> <li>• Folder Path</li> <li>• Group</li> <li>• User</li> <li>• User or Group</li> <li>• Unknown</li> </ul> <p>For an existing alias, the category is a read-only value and cannot be modified.</p>
<b>Value</b>	<p>The value for the category property. Click <b>Get Value</b> to select a value from a list of values associated with the category you previously selected.</p> <p>If you selected <b>Unknown</b> as the category, you must type a value in the Value field.</p>
<b>User Category</b>	<p>A user-defined integer value for the Value property. Optional property.</p>
<b>During DocApp Installation</b>	<p>Select <b>Prompt Alias value</b> to indicate to prompt for the alias value when an application is installed.</p> <p>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.</p>
<b>Description</b>	<p>A description for the alias.</p>

## 10.5 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 11

## Formats

### 11.1 Overview

Format objects define file formats. Documentum CM 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 Documentum CM 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.

### 11.2 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 “[Format properties](#)” on page 293.
4. Click **OK** to save the format or **Cancel** to exit without saving the changes.

**Table 11-1: Format properties**

Field	Description
<b>Name</b>	The name of the format (for example: doc, tiff, or lotmanu).
<b>Default File Extension</b>	The DOS file extension to use when copying a file in the format into the common area, client local area, or storage.

Field	Description
<b>Description</b>	A description of the format.
<b>Com Class ID</b>	The class ID (CLSID) recognized by the Microsoft Windows registry for a content type.
<b>Mime Type</b>	The Multimedia Internet Mail Extension (MIME) for the content type.
<b>Windows Application</b>	The name of the Windows application to launch when users select a document in the format represented by the format object.
<b>Macintosh Creator</b>	Information used internally for managing Macintosh resource files.
<b>Macintosh Type</b>	Information used internally for managing Macintosh resource files.
<b>Class</b>	<p>Identifies the classes or classes of formats to which a particular format belongs. The class property works with all search engines.</p> <p>To assign a class to a format, click <b>Edit</b> to access the Format Class page. Type a value in the <b>Enter new value</b> box and click <b>Add</b>.</p> <p>Two values are used by the full-text indexing system to determine which renditions of a document are indexed:</p> <ul style="list-style-type: none"> <li>• <b>ft_always</b> All renditions of a document are indexed.</li> <li>• <b>ft_preferred</b> If a document has multiple renditions in indexable formats and one format is set to <b>ft_preferred</b>, the rendition in that format is indexed as well as any formats with the class value set to <b>ft_always</b>. If more than one rendition of a document is set to <b>ft_preferred</b>, the first rendition processed for indexing is indexed and the other renditions are not.</li> </ul>
<b>Asset Class</b>	Used by applications. Identifies the kind of asset (video, audio, and so on) represented by this format.
<b>Filename Modifier</b>	The modifier to append to a filename to create a unique file name.
<b>Default Storage</b>	Identifies the default storage area for content files in this format. Click <b>Select</b> to access the Choose a Storage page.

Field	Description
<b>Re-Initialize Server</b>	Select to reinitialize the server so changes occur immediately.
<b>Rich Media</b>	Indicates whether thumbnails, proxies, and metadata are generated for content in this format. You must have OpenText™ Documentum™ Content Management Transformation Services - Media installed to generate the thumbnails, proxies, and metadata.
<b>Hide</b>	Determine whether the format object should appear in the WorkSpace list of formats. Select to hide the object.
<b>Full-Text Indexing</b>	Select to enable the format for full-text indexing.

## 11.3 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.



# Chapter 12

## Types

### 12.1 Managing types

In Documentum Administrator, types are managed on 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 with OpenText™ Documentum™ Content Management High-Volume Server and Documentum CM Server version 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 sysobject type.

Assignment policies determine the correct storage area for content files. A new type inherits a default assignment policy from the nearest supertype in the type hierarchy that has an active assignment policy associated with it. After the type is created, associate a different assignment policy with the type.

*OpenText Documentum Content Management - Server Fundamentals Guide* (EDCCS250400-GGD) provides more information on types. *OpenText Documentum Content Management - Server System Object Reference Guide* (EDCCS250400-ORD) provides complete information on the system-defined object types, including the properties of each type.

## 12.2 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 “[Type properties](#)” on page 298.
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 12-1: Type properties**

Field	Description
Info	

Field	Description
<b>Type Name</b>	The name of the object type. This field is read-only in modify mode.
<b>Model Type</b>	<p>This field is read-only in modify mode.</p> <p>Options are:</p> <ul style="list-style-type: none"> <li>• <i>Standard</i>: This is the default and is for heavy types.</li> <li>• <i>Shareable</i>: Defines a shareable SysObject model type for SysObject supertypes and their subtypes.</li> <li>• <i>Lightweight</i>: 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 available. If selected, the Parent Type, Materialize, and FullText fields become available and the Super Type Name field is not displayed.</li> </ul>
<b>Super Type Name</b>	<p>The name of the supertype. The default supertype is dm_document. This field is:</p> <ul style="list-style-type: none"> <li>• Not available if the Model Type is Lightweight.</li> <li>• Read-only in modify mode.</li> </ul> <p>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.</p>
<b>Default Storage</b>	A default file store for the object type.
<b>Default Group</b>	A default group for the type. Click <b>Select Default Group</b> to access to add or change the default group.
<b>Default Permission Set</b>	A default permission set for the type. Click <b>Select Default Permission Set</b> to add or change the default permission set.

Field	Description
<b>Default Assignment Policy</b>	<p>The system displays the default assignment policy for the type, if there is one. This field appears only when modifying a type and if Content Storage Services is available for the repository.</p> <p>Click the link to access the assignment policy. Use the information in <a href="#">"Assignment policies" on page 345</a> to modify the assignment policy or to remove the type from the assignment policy. Use the instructions in the Assignment Policy section to associate a different policy with a particular type.</p>
<b>Enable Indexing</b>	<p>The system displays the Enable Indexing check box if:</p> <ul style="list-style-type: none"> <li>• 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 check box.</li> <li>• A type and none of its supertypes are registered. The system displays the check box cleared and enabled. You can select the check box to register the type for full-text indexing.</li> <li>• A type is registered and none of its supertypes are registered. The system displays the Enable Indexing check box selected and enabled.</li> <li>• A supertype of the type is registered for indexing. The system displays the Enable Indexing check box selected but disabled. You cannot clear the check box.</li> </ul> <p>The system does not display the Enable Indexing check box when you create a type. You must first create the type and save it.</p> <p>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.</p>

Field	Description
<b>Partitioned</b>	<p>Displays whether a type that can be partitioned is or is not partitioned. This field:</p> <ul style="list-style-type: none"> <li>• Does not appear if the type cannot be partitioned.</li> <li>• Displays <i>False</i> if the type can be partitioned but is not.</li> <li>• Displays <i>True</i> if the type is partitioned.</li> </ul>
<b>Parent Type</b>	<p>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 with OpenText Documentum Content Management (CM) High-Volume Server and if the Documentum CM Server version is 6 or later.</p>
<b>Materialize</b>	<p>This option is available only when creating a type and Model Type is Lightweight. This field is read-only in modify mode.</p> <p>Select one of the following options:</p> <ul style="list-style-type: none"> <li>• <i>Auto materialize</i>: 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.</li> <li>• <i>Materialize on request</i>: 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.</li> <li>• <i>Do not materialize</i>: 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.</li> </ul>
<b>Full Text</b>	<p>This option is available only when creating a type and Model Type is Lightweight. This field is display-only in modify mode.</p> <p>Select one of the following options:</p> <ul style="list-style-type: none"> <li>• No fulltext: This is the default.</li> <li>• Light fulltext: No attributes inherited from the shared parent will be full-text indexed.</li> <li>• Full fulltext</li> </ul>
<b>Attribute</b>	

Field	Description
<b>Attribute Name</b>	The name of the attribute. This field is display-only in modify mode.
<b>Type</b>	The property type.
<b>Size</b>	The size of the property, if the property is the String type.
<b>Inherited</b>	<i>Yes</i> indicates that a property is inherited from a supertype. <i>No</i> indicates that the property is user-defined. You cannot remove a property inherited from the supertype.
<b>Repeating</b>	If selected, the property is a repeating property.

## 12.3 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 check box next to the type's name and click **OK**.

## 12.4 Deleting types

Use the instructions in this section to delete types.

You can only remove a user-defined type from the repository if:

- You are the owner of the type or have superuser privileges.
- The type has no subtypes.
- There are no existing objects of that type in the repository.

You cannot remove system-defined types from the repository. If you delete an object type with an associated assignment policy, the assignment policy is not removed. You can delete it manually.

You cannot delete a shareable type that is shared by a lightweight sysobject. Delete the dependent lightweight objects first.

**To delete a type:**

1. Navigate to **Administration > Types** to access the Types list page.  
A list of existing object types is displayed.
2. Select the type to delete.
3. Select **File > Delete**.  
The type is deleted.

## 12.5 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.

## 12.6 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 with High-Volume Server.

### To convert a type to a shareable object type:

1. Navigate to **Administration > Types** to access the **Types** list page.  
A list of existing object types is displayed.
2. Select the type to share and then select **Tools > Convert to sharable object type**.  
The **Convert Object** page is displayed.
3. Click **OK** to convert the object to a shareable object type or click **Cancel**.

## 12.7 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 with High-Volume Server.

### 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*.

## 12.8 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 with High-Volume Server.

### 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 13

## Storage management

### 13.1 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 (Centera and NetApp SnapLock), blob stores, turbo stores, Atmos 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 with Content Storage Services.

- Migration policies

The Migration Policies area contains pages for creating jobs to move content files among storage areas based on user-defined rules and schedules. These pages only appear with Content Storage Services.

### 13.2 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, OpenText Documentum CM can use this storage system. The first ten storage areas in the repository are displayed in the order in which they were created.

#### 13.2.1 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” on page 308](#) provides information about creating, viewing, or modifying file stores.

### 13.2.1.1 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. “[File store properties](#)” on page 308 describes all file store properties.
5. Click **OK** to save your changes.

**Table 13-1: File store properties**

Field	Description
<b>Info</b>	
<b>Name</b>	The name of the file store. The name must be unique within the repository.
<b>Description</b>	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.
<b>Location</b>	Select the location on the server host.   <b>Caution</b> 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.

Field	Description
<b>Media Type</b>	<p>The media type to store in the storage area. Options are:</p> <ul style="list-style-type: none"> <li>• Regular Content</li> <li>• Thumbnail Content</li> <li>• Streaming Content</li> </ul> <p>Media type cannot be changed for an existing file store.</p>
<b>Base URL</b>	<p>The base URL used to retrieve content directly from a storage area.</p>
<b>Encrypted</b>	<p>Indicates if the files store is encrypted. This option is only available in repositories with Trusted Content Services and cannot be changed for an existing file store.</p>
<b>Make Public</b>	<p>Indicates if the area is accessible to the public with no restrictions.</p>
<b>Add Extension</b>	<p>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.</p>
<b>Require Ticket</b>	<p>Indicates whether the server generates a ticket when returning the URL to a content file.</p>
<b>SurrogateGet Method</b>	<p>Installs a custom SurrogateGet method. This field only displays for an existing file store.</p> <p>To install the method, click <b>Select Method</b> and browse to the method on the server host file system.</p>
<b>Offline Get Method</b>	<p>Indicates whether the server uses an offline Get method. This field only displays for an existing file store.</p>
<b>Status</b>	<p>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.</p>

Field	Description
<b>Digital Shredding</b>	<p>Select to enable digital shredding.</p> <p>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 Trusted Content Services.</p> <p> <b>Caution</b></p> <p>The Documentum Administrator interface for version 6 and later displays the <b>Digital Shredding</b> check box for all file stores. If the file store is a component of a distributed store, files are not digitally shredded even when it appears that digital shredding is enabled for the file store.</p>
<b>Content Compression</b>	<p>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.</p> <p>Content compression is a feature that automatically compresses a file to a smaller size when the file is created. Content compression requires Content Storage Services. You cannot enable content compression after the file store is created.</p>

Field	Description
<b>Content Duplication</b>	<p>Select to enable content duplication checking. This option is only available in repositories with Content Storage Services.</p> <ul style="list-style-type: none"> <li>When <b>Generate content hash values only</b> is selected, for each piece of content checked in to the repository, Documentum CM Server calculates the value needed to determine whether or not it is duplicate content.</li> <li>When <b>Generate content hash values and check for duplicate content</b> is selected, for each piece of content checked in to the repository, Documentum CM Server calculates the value needed to determine whether or not it is duplicate content and then checks for duplicate content.</li> </ul> <p>Content duplication minimizes the amount of content file duplication in the file store. Content duplication checking requires Content Storage Services.</p> <p>You cannot enable content duplication checking after the file store is created.</p>
<b>Space Info</b>	The Space Info tab only displays for an existing file store.
<b>Active Space/Files</b>	The space used by the file store and the number of files.
<b>Orphaned Space/Files</b>	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 /y 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.

► **Example 13-1:**

```
C:> copy C:\<OldLocation>\*.* C:\<NewLocation>
```



If the target directory does 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.

► **Example 13-2:**

```
UPDATE "dm_location" OBJECT  
SET "file_system_path" = 'C:\<NewLocation>'  
where object_name='loc1'
```



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:** OpenText recommends that you use Documentum Administrator to perform the DQL statements.

### 13.2.1.2 Configuring NAS file stores

This section describes the instructions to configure Data Domain and Isilon NAS file stores.

Before configuring, ensure the following for Windows:

- Documentum CM Server host and NAS storage host should be in same domain.
- Domain Administrator only can install Documentum CM Server on the Documentum CM Server host.

#### To configure NAS file stores:

1. Log in to the Documentum CM Server Windows host as the domain administrator.
2. Install Documentum CM Server on the Documentum CM Server host. *OpenText Documentum Content Management - Server and Server Extensions Installation Guide (EDCSY250400-IGD)* contains the installation instructions.
3. Once the Documentum CM Server installation is complete, you will be prompted to configure the repository using the Documentum CM 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: NAS storage device NFS share path is mounted on the Linux 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 Documentum CM Server configuration program and complete it. *OpenText Documentum Content Management -*

*Server and Server Extensions Installation Guide (EDCSY250400-IGD)* contains the detailed instructions.

After the Documentum CM Server configuration program is complete, the NFS file store share is created.

## 13.2.2 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 OpenText Documentum CM 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 Linux hosts, the linked store contains a logical link to the actual storage area.

[“Creating, viewing, or modifying linked stores” on page 314](#) provides information about creating viewing or modifying linked stores.

### 13.2.2.1 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 > Storage 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 [“Linked store properties” on page 314](#).
5. Click **OK** to save your changes.

**Table 13-2: Linked store properties**

Field	Description
<b>Name</b>	The name of the storage object. This name must be unique within the repository.
<b>Location</b>	The name of the directory containing the logical link.

Field	Description
<b>Linked Store</b>	The name of the storage area to which the link is pointing.
<b>Use symbolic links</b>	If selected, symbolic links are used.
<b>Get Method</b>	To install a custom SurrogateGet, click <b>Select Method</b> and browse to the method on the server host file system.  This option only appears if you are modifying an existing linked store.
<b>Offline Get Method</b>	Select to use an offline Get method.  This option only appears if you are modifying an existing linked store.
<b>Status</b>	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.

### 13.2.3 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” on page 316](#) provides information about creating, viewing, or modifying blob stores.

### 13.2.3.1 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 > Storage 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. “[Blob store properties](#)” on page 316 describes all blob store properties.
5. Click **OK** to save your changes.

**Table 13-3: Blob store properties**

Field	Description
<b>Name</b>	The name of the storage object. This name must be unique within the repository and must conform to the rules governing type names.
<b>Content Type</b>	Valid values are: <ul style="list-style-type: none"><li>• <b>ASCII</b></li><li>• <b>8-bit Characters</b></li></ul>
<b>Get Method</b>	To install a custom SurrogateGet, click <b>Select Method</b> and browse to the method on the server host file system.  This option only displays for existing blob stores.
<b>Offline Get Method</b>	Select to use an offline Get method.  This option only displays for existing blob stores.

Field	Description
Status	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.

## 13.2.4 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.

### 13.2.4.1 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 > Storage 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 “[Mount point properties](#)” on page 317.
5. Click **OK** to save your changes.

**Table 13-4: Mount point properties**

Field	Description
<b>Name</b>	The name of the mount point object.  Some names, such as “events” or “common”, are reserved for Documentum CM Server use.
<b>Host Name</b>	The host name for the machine on which this directory resides.

Field	Description
<b>File System Path</b>	<p>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.</p> <p>For example, if the server is on a Windows NT machine, the location must be expressed as a Windows NT path.</p> <div style="border: 1px solid #ccc; padding: 5px; margin-top: 10px;">  <b>Caution</b>            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.         </div>
<b>Security</b>	<p>The security level for this directory location. Options are:</p> <ul style="list-style-type: none"> <li>• Public Open</li> <li>• Public</li> <li>• Private</li> </ul> <p>The default value is Private.</p>
<b>Unix Preferred Alias</b>	<p>Set to the directory name used to mount the directory.</p>
<b>Macintosh Preferred Alias</b>	<p>Set to the volume name chosen for the mounted directory.</p> <p>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.</p>
<b>Windows Preferred Alias</b>	<p>Set to the alias drive letter used to mount the directory.</p> <p>For example, t:\ or k:\ .</p>
<b>Comments</b>	<p>Enter any comments about the mount point.</p>

### 13.2.5 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 Documentum CM 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. OpenText Documentum CM 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” on page 320](#) provides information about creating, viewing, or modifying external stores.

*OpenText Documentum Content Management - Server and Server Extensions Installation Guide (EDCSY250400-IGD)* provides more information about external XML file stores.

### 13.2.5.1 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 > Storage 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.  
[“External store properties” on page 320](#) describes all distributed store properties.

**Table 13-5: External store properties**

Field	Description
<b>Info</b>	
<b>Name</b>	The name of the new external store.
<b>Windows</b>	Indicates the plug-in that is used on the Windows platform.
<b>Solaris</b>	Indicates the plug-in that is used on the Solaris platform.

Field	Description
<b>Aix</b>	Indicates the plug-in that is used on the Aix platform.
<b>HP-UX</b>	Indicates the plug-in that is used on the HP-UX platform.
<b>Macintosh</b>	Indicates the plug-in that is used on the Macintosh platform.
<b>Linux</b>	Indicates the plug-in that is used on the Linux platform.
<b>HP-UX-Itanium</b>	Indicates the plug-in that is used on the HP-UX-Itanium platform.
<b>Current Client Root</b>	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.
<b>Client Root</b>	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.  <b>Client Root:</b> Click <b>Browse</b> and select a client root.
<b>Server</b>	The Server tab only displays for external file stores.
<b>Add</b>	Click <b>Add</b> or select the server on which the external file store resides, then click <b>Edit</b> to access the <b>Choose a server config</b> page.
<b>Server</b>	The name of the server where the external store resides.
<b>Location</b>	The location object that points to the external file store. Click <b>Select Location</b> to select a location object.
<b>Path</b>	Specifies the file system path to the external file store. The path displays automatically after you selected the location object.

### 13.2.5.2 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**.

### 13.2.6 NetApp SnapLock stores

A Network Appliance SnapLock (NetApp SnapLock) store stores large amounts of unchanging data such as email archives. NetApp SnapLock 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 a Centera store. You can define a retention date or, with Documentum CM 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 Documentum CM Server version 5.3 SP6 or later
- A SnapLock storage device
- A connector

[“Creating, viewing, or modifying NetApp SnapLock stores” on page 323](#) provides information about creating, viewing, or modifying NetApp SnapLock stores.

### 13.2.6.1 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 > Storage 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. “[NetApp SnapLock store properties](#)” on page 323 describes all NetApp SnapLock store properties.
5. Click **OK** to save your changes.

**Table 13-6: NetApp SnapLock store properties**

Field	Description
Name	The name of the NetApp SnapLock store.
Description	A description of the NetApp SnapLock store.

Field	Description
<b>Plug-in Name</b>	<p>The name of the plug-in for the NetApp SnapLock store. Options are:</p> <ul style="list-style-type: none"> <li>• <b>Default Plugin:</b> Set to the default CSEC plugin and NetApp Snaplock Connector respectively.</li> <li>• <b>Select Plugin:</b> Select the plugin you want to use.</li> </ul> <p>When a repository is created, a default plug-in object is created. If the plug-in object is deleted from the repository, no plug-in is displayed. Use the instructions in <a href="#">“Creating or modifying plug-ins” on page 342</a> to create a new plug-in object with the content of the plug-in object set as follows:</p> <ul style="list-style-type: none"> <li>– Windows: %DM_HOME%\bin\emcplugin.so</li> </ul> <p>When a repository is created, a default plug-in object is created. If the plug-in object is deleted from the repository, no plug-in is displayed. Use the instructions in <a href="#">“Creating or modifying plug-ins” on page 342</a> to create a new plug-in object with the content of the plug-in object set as follows:</p> <ul style="list-style-type: none"> <li>• Windows: %DM_HOME%\bin\emcplugin.so</li> </ul>
<b>Snaplock Volume Path</b>	The directory path of the NetApp SnapLock storage system.
<b>Enable Content Compression</b>	<p>Specifies whether content compression is used. Select this option to compress all content in the store.</p> <p>Compression cannot be modified for existing NetApp SnapLock stores.</p>
<b>Configure Retention Information</b>	<p>Enables content retention.</p> <p>Content retention cannot be modified for existing NetApp SnapLock store.</p>
<b>Retention Attribute Name</b>	<p>The name of the retention attribute. The value must <i>not</i> be one of the values specified as a content attribute name.</p> <p>The retention attribute name cannot be modified for an existing NetApp SnapLock store.</p>

Field	Description
<b>Fixed Retention</b>	<p>Specifies a fixed value for the retention property value, as follows:</p> <ul style="list-style-type: none"> <li>• <b>Choose a retention period:</b> 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.</li> <li>• <b>Choose default retention days:</b> Select and then type the number of retention days.</li> </ul> <p>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.</p>
<b>Event Based Retention</b>	<p>When Configure Retention Information is selected, the system automatically selects and inactivates this check box to prevent changing the event based retention option status.</p>
<b>Application Provides Retention</b>	<p>Requires that a client application supplies the retention date when content is saved to the NetApp SnapLock store.</p>

### 13.2.7 Centera stores

An Centera store is a retention store for large amounts of unchanging data such as email archives or check images. Centera requires Content Services for EMC Centera (CSEC).

In a Centera store:

- Store metadata values with a piece of content.
- Store files created on Macintosh platforms.

Both, Documentum CM Server and Foundation Java API must be on version 6.7 or later and there is no backward compatibility to older versions of Documentum CM Server and Foundation Java API. Any attempt to store resource forks into a Centera store using either an earlier Documentum CM Server or Foundation Java API version results in an exception/error message.

- Define a retention date or, with Documentum CM 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.

Documentum CM 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 Documentum CM Servers are running on the same computer, the Centera store plug-in must be in a file store.
- If the Documentum CM Servers are running on different hosts, the Centera store plug-in must be stored in a file store that is shared by all Documentum CM Server instances or in a distributed store in which each Documentum CM Server has at least one component defined as a near store.

[“Creating, viewing, or modifying Centera stores” on page 326](#) provides information about creating, viewing, or modifying Centera stores.

### 13.2.7.1 **Creating, viewing, or modifying Centera stores**

To create a Centera store, you must know the connection string of the Centera storage system.

**To create, view, or modify a Centera store:**

1. Connect to the repository, where you want to create, view or modify a Centera store.
2. Select **Administration > Storage Management > Storage**.  
The **Storage** list page displays.
3. Do one of the following:
  - To create a Centera store, select **File > New > EMC Centera Store**.
  - To view or modify an existing 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 Centera store. [“EMC Centera store properties” on page 327](#) describes all Centera store properties.
5. Click **OK** to save your changes.

**Table 13-7: EMC Centera store properties**

<b>Field</b>	<b>Description</b>
<b>Name</b>	The name of the Centera store.
<b>Description</b>	A description of the Centera store.
<b>Plug-in Name</b>	<p>Specifies the plug-in that is used for the Centera store. Select one of the following options:</p> <ul style="list-style-type: none"> <li>• <b>Default Plugin:</b> Set to the default CSEC plugin and NetApp Snaplock Connector respectively.</li> <li>• <b>Select Plugin:</b> Select the plugin you want to use.</li> </ul> <p>When a repository is created, a default plug-in object for CSEC is created. If the plug-in object is deleted from the repository, no plug-in is displayed. Use the instructions in <a href="#">“Creating or modifying plug-ins” on page 342</a> to create a new plug-in object with the content of the plug-in object set as follows:</p> <ul style="list-style-type: none"> <li>• Windows: %DM_HOME%\bin\emcplugin.dll</li> <li>• Linux: \$DM_HOME/bin/libemcplugin.so</li> </ul>
<b>Storage Parameters</b>	<p>Specifies the storage parameters, such as the connection string, C-clip buffer size, and embedded blob storage.</p> <p>Click <b>Edit</b> to configure storage parameters, as described in <a href="#">“Defining the storage parameters for a Centera store” on page 329</a>.</p>
<b>Enable Content Compression</b>	<p>Specifies whether content compression is used. Select this option to compress all content in the store.</p> <p>Compression cannot be modified for existing Centera stores.</p>
<b>Configure Retention Information</b>	<p>Enables content retention.</p> <p>Content retention cannot be modified for existing Centera stores.</p>
<b>Retention Attribute Name</b>	<p>The name of the retention attribute. The value must <i>not</i> be one of the values specified as a content attribute name.</p> <p>The retention attribute name cannot be modified for an existing Centera store.</p>

Field	Description
<b>Fixed Retention</b>	<p>Specifies a fixed value for the retention property value, as follows:</p> <ul style="list-style-type: none"> <li>• <b>Choose a retention period:</b> 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.</li> <li>• <b>Choose default retention days:</b> Select and then type the number of retention days.</li> </ul> <p>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.</p>
<b>Event Based Retention</b>	<p>When Configure Retention Information is selected, the system automatically selects and inactivates this check box to prevent changing the event based retention option status.</p>
<b>Application Provides Retention</b>	<p>Requires that a client application supplies the retention date when content is saved to the Centera store.</p>
<b>Add</b>	<p>Click <b>Add</b> to add a content attribute, or select an attribute from the list and click <b>Edit</b>. The Content Attribute window displays.</p> <p>Enter or modify the following information:</p> <ul style="list-style-type: none"> <li>• <i>Attribute Name:</i> The name of the content attribute. The content 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.</li> <li>• <i>Attribute Description:</i> A brief description of the content attribute.</li> </ul>

### 13.2.7.2 Defining the storage parameters for a Centera store

Use the instructions in this section to add or modify storage parameters for the Centera store.

#### To define the storage parameters for a 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 Centera storage system.

The connection string has the following format:

```
<IP_address>|<host_name>{,<IP_address>|<host_name>}?<Centera_profile>
```

where:

- *IP\_address* is the IP address of the Centera host.
- *host name* 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 Documentum CM Server host machine and the specified directory must be readable by the Documentum CM 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:

```
outConnectionStrings [0] = 10.241.35.27?name=profA,secret=  
foooutConnectionStrings [1] = 10.241.35.28?name=profA,secret=  
foooutConnectionStrings [2] = 10.241.35.27?name=profB,secret=  
baroutConnectionStrings [3] = 10.241.35.28?name=profB,secret=  
baroutConnectionStrings [4] = 10.241.35.110?path=C:\Temp\  
auth.xmloutConnectionStrings [5] = 10.241.35.111?path=C:\Temp\auth.xml
```

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 Documentum CM 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 Documentum CM Server writes.
- The secondary *<cluster\_id>* is the name or IP address of the Centera cluster from which the Documentum CM 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, Documentum CM 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 Linux platforms.

5. Use the up and down arrows to sort the storage parameters.



### Caution

If you have entered multiple parameters, the Centera connection string must be in the first position.

6. When finished, click **OK**.

#### 13.2.7.3 Defining Centera store content attributes

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 a 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.

## 13.2.8 Atmos stores

An Atmos store is a software storage system that consists of several distributed services running on a network of connected hardware nodes. Each node is attached to one or more disk enclosures. The nodes run a collection of services to store, retrieve, categorize, and manage the data in the system or cloud.

Documentum CM Server uses the Accelerated Content Services connector to communicate with the Atmos store. The Accelerated Content Services module supports storing and retrieving of content through an HTTP interface.

[“Creating, viewing, or modifying Atmos stores” on page 332](#) provides information about creating, viewing, or modifying Atmos stores.

### 13.2.8.1 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. [“Atmos store properties” on page 332](#) describes all Atmos store properties.
5. Click **OK** to save your changes.

**Table 13-8: Atmos store properties**

Field	Description
Name	The name of the Atmos store. The name must be unique within the system. The name of an existing Atmos store cannot be modified.
URL	The URL the server uses to communicate with the Atmos store.

Field	Description
<b>Full Token ID</b>	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.
<b>Shared Secret</b>	The password of the user accessing the Atmos store.

### 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 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:

MBqhzSzhZJCQHE9U4RBK9ze3K7U=

#### 13.2.9 Amazon S3 stores

Amazon S3 is a highly durable and available store that can be used to reliably store application content such as media files, static assets and user uploads. It allows you to offload your entire storage infrastructure and offers better scalability, reliability, and speed than just storing files on the file system. You can use it as a content store for Documentum CM Server.

A store plugin is used to make the communication between OpenText Documentum CM and External Store (S3). The store plugin implements the contract defined by Foundation Java API store plugin interface and provides content transfer capability. This implementation acts as a bridge or adaptor between Foundation Java API store plugin and the Amazon S3 RESTful Java API binding.

Once it is configured, the store is accessible as any other Documentum CM Server store. A new TBO is created for the plugin. The dm\_s3\_store object cannot be updated once it is created. All the contents uploaded to the Amazon S3 store have an unique key. This key is derived from the content-id.

“Creating, viewing, or modifying S3 stores” on page 334 provides the detailed information.

### 13.2.9.1 Creating, viewing, or modifying S3 stores

#### To create, view, or modify S3 store:

1. Connect to the repository, where you want to create, view, or modify the S3 store.
2. Select **Administration > Storage Management > Storage**.  
The **Storage** list page appears.
3. Do one of the following:
  - To create a S3 store, select **File > New > S3 Store**.
  - To view or modify an existing S3 store, select a S3 store, then select **View > Properties > Info**.

Some of the fields for an existing S3 store cannot be modified. “S3 store properties” on page 334 describes all S3 store properties.

4. Click **OK** to save the changes.

**Table 13-9: S3 store properties**

Field	Description
<b>Name</b>	The name of the S3 store. The name must be unique within the system. The name of an existing S3 store cannot be modified.
<b>URL</b>	The URL that the server uses to communicate with the S3 store. The URL format is <code>http://&lt;X.X.X.X&gt;/&lt;&lt;BUCKET&gt;&gt;</code> .
<b>Access Key ID</b>	The user name of the user accessing the S3 store. Use the S3 Tenant Owner as the Access Key ID. This is an optional field.
<b>Shared Secret</b>	The password of the user accessing the S3 store. Use the Object Access Key as the Shared Secret. This is an optional field.
<b>Encrypted</b>	The encrypted form of the store. The default value is <b>No</b> .
<b>Proxy Host</b>	The IP address of the proxy server. This is an optional field.
<b>Proxy Port</b>	The port reserved for the proxy server. This is an optional field.
<b>Region</b>	The region where S3 bucket is configured. This is an optional field.

Field	Description
<b>Query Parameter</b>	The URL query parameter that the corresponding S3 store vendor expects for extending retention. This is specific to the compatible store. This is an optional field.
<b>Retention Header Name</b>	Header used for specifying the new retention date. The date format must be in accordance to the ISO 8601 format (YYYYMMDDThhmmssZ). This is specific to the compatible store. This is an optional field.
<b>Mode</b>	Retention mode that applies to different levels of protection. This is an optional field used for the <b>AmazonS3</b> vendor only. Valid values are: <ul style="list-style-type: none"> <li>• null</li> <li>• COMPLIANCE</li> <li>• GOVERNANCE: This is the default value for Amazon S3.</li> </ul>
<b>Vendor</b>	Specifies the storage vendor. This is an optional field. Valid values are: <ul style="list-style-type: none"> <li>• null</li> <li>• AmazonS3</li> <li>• NetAppStorageGRID</li> <li>• HCP</li> <li>• IBMCOS</li> <li>• EMCECS</li> </ul>

### 13.2.10 OpenStack Swift stores

The OpenStack object store, known as Swift, offers cloud storage software to store and retrieve lots of data with a simple API. It is optimized for durability, availability, and concurrency across the entire data set. It is ideal for storing unstructured data that can grow without bound. You can use OpenStack Swift as a content store for Documentum CM Server.

A store plugin using REST APIs is used to allow Documentum CM Server to configure OpenStack as a data store. This plugin is available as `dm_swift_store` type in Documentum CM Server.

Once it is configured, the store is accessible as any other Documentum CM Server store. A new TBO is created for the plugin. All the contents uploaded to the OpenStack store have an unique key. This key, which is in the form of a UNIX path, is derived from the content-id.

[“Creating, viewing, or modifying OpenStack Swift stores” on page 336](#) provides the detailed information.

### 13.2.10.1 Creating, viewing, or modifying OpenStack Swift stores

#### To create, view, or modify OpenStack Swift store:

1. Connect to the repository, where you want to create, view, or modify the OpenStack store.

2. Select **Administration > Storage Management > Storage**.

The **Storage** list page appears.

3. Do one of the following:

- To create a OpenStack Swift store, select **File > New > OpenStack Swift Store**.
- To view or modify an existing OpenStack Swift store, select a OpenStack Swift store, then select **View > Properties > Info**.

Some of the fields for an existing OpenStack Swift store cannot be modified.

["OpenStack Swift store properties" on page 336](#) describes all OpenStack Swift store properties.

4. Click **OK** to save the changes.

**Table 13-10: OpenStack Swift store properties**

Field	Description
<b>Name</b>	The name of the OpenStack Swift store. The name must be unique within the system. The name of an existing OpenStack Swift store cannot be modified.
<b>Authentication endpoint URL</b>	The URL that the server uses to communicate with the OpenStack Swift store. For example, <a href="http://10.0.0.1:35357/v2.0">http://10.0.0.1:35357/v2.0</a>
<b>Account Owner</b>	The user name of the user accessing the OpenStack Swift store.
<b>Password</b>	The password of the user accessing the OpenStack Swift store.
<b>Container</b>	The name of the container to store the content.
<b>Region</b>	The name of the preferred region to store the content. This is an optional field.

## 13.2.11 REST stores

Documentum CM Server supports Azure Blob and Google Cloud storage types as REST object store. You can configure REST store as a file store. The two main components are REST store plug-in and Accelerated Content Services connector.

*OpenText Documentum Content Management - Server Administration and Configuration Guide (EDCCS250400-AGD)* contains more information.

“Creating or viewing REST stores” on page 337 provides the detailed information.

### 13.2.11.1 Creating or viewing REST stores

**To create or view REST store:**

1. Connect to the repository, where you want to create or view the REST store.
2. Select **Administration > Storage Management > Storage**.
3. On the **Storage** list page, do one of the following:
  - To create a REST store, select **File > New > Rest Store**.
  - To view an existing REST store, select a REST store, and then select **View > Properties > Info**.

“REST store properties” on page 337 describes all REST store properties.

4. Click **OK** to save the changes.

**Table 13-11: REST store properties**

Field	Description
<b>Name</b>	The name of the REST store. The name must be unique within the system. The name of an existing REST store cannot be modified.
<b>URL</b>	The URL that the server uses to communicate with the REST store.
<b>Store Type</b>	Specifies the storage type. Valid values are: <ul style="list-style-type: none"> <li>• Azure Blob</li> <li>• GCP Store</li> </ul>
<b>Access Key ID</b>	The user name of the user accessing the REST store. Use the REST Tenant Owner as the Access Key ID. This field is applicable only for Azure Blob store.
<b>Shared Secret</b>	The password of the user accessing the REST store. Use the Object Access Key as the Shared Secret. This field is applicable only for Azure Blob store.

Field	Description
<b>Service Account</b>	Click <b>Browse</b> and select the Google Cloud storage type service account credentials in the JSON format. This field is applicable only for Google Cloud store.
<b>Encrypted</b>	Specifies if content is encrypted.
<b>Compression</b>	Specifies if content compression is enabled.
<b>De-duplication</b>	Specifies if de-duplication is enabled.

### 13.2.12 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 combination 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.

*OpenText Documentum Content Management - Server and Server Extensions Installation Guide (EDCSY250400-IGD)* describes how to implement and administer a distributed storage area. *OpenText Documentum Content Management - Server System Object Reference Guide (EDCCS250400-ORD)* lists the properties defined for the distributed store object type.

[“Creating, viewing, or modifying distributed stores” on page 338](#) provides information about creating, viewing, or modifying distributed stores.

#### 13.2.12.1 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 > Storage 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. “[Distributed store properties](#)” on page 339 describes all distributed store properties.
5. Click **Finish** or **OK** to save your changes.

**Table 13-12: Distributed store properties**

Field	Description
<b>Info</b>	
<b>Name</b>	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.
<b>Fetch Content Locally Only</b>	Indicates whether the server fetches content locally or from far stores that are not available locally.
<b>Get Method</b>	<p>To install a custom SurrogateGet, click <b>Select Method</b> to access the Choose a method page to select a method on the server host file system.</p> <p>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, OpenText Documentum CM provides the surrogate get feature, which allows the server to automatically replicate content when a fetch fails.</p> <p>Implement this feature using the surrogate get method provided by default with the Documentum CM Server system administration tool suite (named <code>dm_SurrogateGet</code>), or write your own surrogate get program. If you write your own, fill in the method name here.</p>

Field	Description
<b>Offline Get Method</b>	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.
<b>Status</b>	Indicates whether the storage area is on line, off line, or read only.
<b>Components</b>	
<b>Add</b>	Adds stores to the distributed store.  Click <b>Add</b> . The <b>Choose a storage:</b> 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.
<b>Remove</b>	Removes stores from the distributed store.  Select a store in the store list and click <b>Remove</b> to remove the store from the distributed store.

### 13.2.13 Locations

The directories that a Documentum CM 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” on page 340](#) provides information on creating or modifying locations.

#### 13.2.13.1 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 > Storage 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 “[Location object properties](#)” on page 341.
5. Click **OK** to save your changes.

**Table 13-13: Location object properties**

Field	Description
<b>Name</b>	<p>The name of the location object.</p> <p>Some names, such as “events” or “common”, are reserved for Documentum CM Server use.</p>
<b>Choose a Mount Point for this Location</b>	<p>Identifies the mount point underneath which this location resides. Use the name of the mount point object that describes the mount point.</p>
<b>Mount Point Path</b>	<p>Specifies the mount point path. Valid values are:</p> <ul style="list-style-type: none"> <li>• <i>Existing</i>: Uses the current mount point path. Select <b>Null</b> to specify that the mount point is not shared, or select <b>share</b> to use this mount point as a shared mount point.</li> <li>• <i>Create Mount Point Path</i>: Select to create a mount point path, then click <b>Select Path</b> to browse to a mount point on the file system.</li> </ul>
<b>Path</b>	<p>Specifies the file system or UNC path.</p> <ul style="list-style-type: none"> <li>• <i>File System Path</i>: 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.</li> <li>• <i>UNC</i>: Indicates the UNC path.</li> </ul> <div data-bbox="966 1600 1057 1706"> </div> <p><b>Caution</b></p> <p>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.</p>

Field	Description
<b>Path Type</b>	Indicates whether the location points to a directory or file.
<b>Security Type</b>	The security level for the directory or file. Valid values are: <ul style="list-style-type: none"><li>• publicopen</li><li>• public</li><li>• private</li></ul> If the security type is not set, the default value is the security level of the referencing object, such an associated storage object.

### 13.2.14 Plug-ins

A plug-in is a shared library (on Linux systems) or DLL file (on Windows systems) for retrieving content when an external store is in use.

You must create the plug-in. OpenText Documentum CM provides code for sample plug-ins in the DM\_HOME/unsupported/plugins directory. The sample plug-ins are examples and are not supported.

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” on page 342](#) provides information on creating or modifying plug-ins.

#### 13.2.14.1 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 > Storage 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 [“Plug-in properties” on page 343](#).

5. Click **OK** to save your changes.

**Table 13-14: Plug-in properties**

Field	Description
<b>Name</b>	The name of the plug-in object.
<b>Hardware Platform</b>	Specifies one or more hardware platforms on which the plug-in can run.  Click <b>Edit</b> to access the <b>Hardware Platforms</b> page. Enter the hardware type in the <b>Enter a new value</b> field, then click <b>Add</b> . When all types are entered, click <b>OK</b> .
<b>Operating System</b>	Specifies one or more operating systems on which the plug-in can run.  Click <b>Edit</b> to access the <b>Host Machine</b> page. Enter the operating system in the <b>Enter a new value</b> field, then click <b>Add</b> . When all operating systems are entered, click <b>OK</b> .
<b>Type</b>	Select a file type. Options are: <ul style="list-style-type: none"> <li>• <b>DLL (Windows)</b></li> <li>• <b>SO (Linux)</b></li> </ul>
<b>Usage</b>	Type a comment on how the plug-in is used.

### 13.2.15 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.

### 13.2.16 Setting or updating a retention date or retention period

A 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. Documentum CM 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**.

## 13.3 Assignment policies

Assignment policies are sets of rules that Foundation Java API-based applications apply to determine the correct file store or retention store for each new content file added to the repository. Assignment policies require Content Storage Services (CSS). Any client application built on Foundation Java API 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](#)” on page 349 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). OpenText Documentum CM 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 Foundation Java API 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 Foundation Java API 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.

### 13.3.1 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

### 13.3.2 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 with Content Storage Services.

#### 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 “[Assignment policy properties](#)” on page 348.
4. Click **Finish** to create the policy or **Cancel** to exit without creating the policy.

**Table 13-15: Assignment policy properties**

<b>Field</b>	<b>Description</b>
<b>Name</b>	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.
<b>Description</b>	A description of the policy. Optional property.
<b>Status</b>	Specifies whether the assignment policy is active. The default status is <b>Inactive</b> . Select <b>Active</b> to enable the policy and automatically validate the rule syntax. The validation process does not check whether property names in the rules are valid.
<b>Validate all of the rules defined for this policy</b>	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 check box is selected and grayed out.  If the policy is created in the inactive state, optionally clear the check box.
<b>Object types</b>	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 <b>Select</b> then select the object types to which the policy applies and click <b>&gt;</b> .
<b>Create/Edit Rules</b>	Specifies the rules for storing content.
<b>Standard Rule</b>	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.
<b>Add Criteria</b>	Click to add additional conditions to the rule.  A standard rule can have up to five criteria.
<b>Insert Rule</b>	Click to insert the completed rule.

Field	Description
<b>Cancel Rule</b>	Click to delete text that has been entered in the text box.
<b>Custom Rule</b>	Type the custom rule in the text box.  “ <a href="#">Custom assignment policy rule examples</a> ” on page 349 provides more information on custom rules and examples of custom rule syntax.
<b>Policy Rules</b>	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 <b>Up</b> and <b>Down</b> links. Edit or delete a rule by clicking the associated <b>Edit</b> and <b>Remove</b> links.

### 13.3.3 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.

### 13.3.4 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 Foundation Java API’s `IDfSysObject`, such as `getString()`, `getInt()`, or `getRepeatingString()`.

Custom rules follow Java syntax for the conditional statement in the rule. The following are examples of valid custom rules:

 **Example 13-3: 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, contact OpenText Global Technical Services.

### 13.3.5 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 associate 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**.

### 13.3.6 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 check boxes 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.

## 13.4 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 (Centera or NetApp SnapLock).

Migration policies are jobs that execute the MIGRATE\_CONTENT administration method. The conditions are stored as job arguments. Content Storage Services (CSS) is required to create content migration jobs.

### 13.4.1 Creating, viewing, or modifying migration policies

Migration policies can be created and used only in repositories with Content Storage Services.

#### 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 “[Migration policy Info tab properties](#)” on page 352.
4. Click **Next** or click the **Schedule** tab to enter migration policy scheduling information, as described in “[Configuring a migration policy schedule](#)” on page 352.
5. Click **Next** or click the **Rules** tab to enter migration policy rules, as described in “[Configuring migration policy rules](#)” on page 353.
6. Click **Next** or click the **SysObject** tab to enter SysObject information, as described in “[Migration policy SysObject tab properties](#)” on page 355.
7. Click **Finish**.

**Table 13-16: Migration policy Info tab properties**

<b>Field</b>	<b>Description</b>
<b>Name</b>	The name of the job. Mandatory property.
<b>Job Type</b>	The type of job. Optional property. The default value is <b>Content</b> .
<b>Trace Level</b>	The trace level from 0 (no tracing) to 10 (a debugging level of tracing).
<b>Designated Server</b>	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 <b>Any Running Server</b> .
<b>State</b>	Specifies whether the policy is active or inactive. The default value is <b>Active</b> .
<b>Options</b>	
<b>Deactivate on Failure</b>	Select to deactivate the job after a run fails to execute correctly.
<b>Run after Update</b>	Select to run the job immediately after it was updated.
<b>Save if Invalid</b>	Select to save the job even if it is invalid.

#### 13.4.1.1 Configuring a migration policy schedule

The migration policy schedule determines when the migration job is executed.

**Table 13-17: Migration policy Schedule tab properties**

<b>Field</b>	<b>Description</b>
<b>Next Run Date and Time</b>	Specifies the next start date and time for the job. The default is the current date and time.
<b>Repeat</b>	Specifies the time interval in which the job is repeated.
<b>Frequency</b>	Specifies how many times the job is repeated. 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.
<b>End Date and Time</b>	Specifies the end date and time for the job. The default end date is 10 years from the current date and time.

Field	Description
After	Specifies the number of invocations after which the job becomes inactive.

### 13.4.1.2 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 “[Migration policy Rules tab properties](#)” on page 353.

**Table 13-18: Migration policy Rules tab properties**

Field	Description
<b>Selected Objects</b>	
Simple selection	Creates a migration rule based on preset values, such as format, creation date, modification date, access date, or size.
Move objects where	<p>Specifies which objects to move. Select one of the criteria from the drop-down list, as follows:</p> <ul style="list-style-type: none"> <li>• <b>format:</b> Migrates objects of a particular format. Click <b>Select</b> and then select the correct format.</li> <li>• <b>created:</b> Migrates objects according to creation date.</li> <li>• <b>modified:</b> Migrates objects according to their modification date.</li> <li>• <b>accessed:</b> Migrates objects according to the date they were last accessed.</li> <li>• <b>size:</b> Migrates objects according to their size in bytes. Enter the number of bytes.</li> </ul> <p>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:</p> <ul style="list-style-type: none"> <li>• <b>Exactly:</b> Migrates objects modified exactly the number of days before.</li> <li>• <b>More than:</b> Migrates objects modified more than the number of days before.</li> <li>• <b>Less than:</b> Migrates objects modified less than the number of days before.</li> </ul>

Field	Description
<b>Renditions to include</b>	Specifies whether to migrate <b>Primary</b> or <b>Secondary</b> renditions or both. The rendition option is only available in conjunction with the created, modified, or accessed selection criteria.
<b>DQL query selection</b>	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.
<b>Move specified type</b>	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.
<b>Move content objects only</b>	Select to migrate the content associated with content objects (dmr_content).
<b>Where</b>	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.
<b>Renditions to include</b>	If you selected <b>Move specified types</b> , select to migrate <b>Primary</b> or <b>Secondary</b> renditions or both.
<b>Move options</b>	
<b>Target Store</b>	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 (Centera and NetApp SnapLock).
<b>Batch Size</b>	The number of content files to include in a single transaction during the migration operation. The default value is 500.
<b>Maximum Count</b>	The maximum number of content files to transfer. To specify an unlimited number of documents, type a zero [0] or leave the field blank.

Field	Description
<b>Content Migration Threads</b>	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 with Content Storage Services on Documentum CM Server. The Content Migration Threads value cannot exceed the Maximum Content Migration Threads value in the server configuration object (dm_server_config).

### 13.4.2 Configuring migration policy SysObject information

The SysObject information typically consists of metadata associated with the object.

**Table 13-19: Migration policy SysObject tab properties**

Field	Description
<b>Title</b>	The title of the object.
<b>Subject</b>	The subject of the object.
<b>Keywords</b>	Keywords that describe the object. Click <b>Edit</b> to access the Keywords page. Enter a new keyword in the <b>Enter new value</b> box and click <b>Add</b> .
<b>Authors</b>	The author of the object. Click <b>Edit</b> to access the Authors page. Type a new author in the <b>Enter new value</b> box and click <b>Add</b> .
<b>Owner Name</b>	The owner of the object. Click <b>Edit</b> to access the Choose a user page and select an owner.
<b>Show more</b>	Click to view more SysObject properties of the migration policy.

### 13.4.3 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.

#### 13.4.4 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, click **Finish**.

# Chapter 14

## Content delivery

### 14.1 Content delivery services

Documentum Interactive Delivery Services and Documentum Interactive Delivery Services Accelerated 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 Documentum CM 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, IDS 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.

*OpenText Documentum Interactive Delivery Services Accelerated Installation Guide* and *OpenText Documentum Interactive Delivery Services Accelerated User Guide* documentation provides additional product information.

*OpenText Documentum Interactive Delivery Services Installation Guide* and *OpenText Documentum Interactive Delivery Services User Guide* documentation provides additional product information.

### 14.2 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 14-1: Content delivery configuration information**

Field	Description
<b>Initial Publishing Date</b>	The date documents were first published using this configuration.
<b>Refresh Date</b>	The date of the last successful full refresh of the content delivery configuration.
<b>Last Increment Date</b>	The date of the last successful incremental publish event for the content delivery configuration.
<b>Increment Count</b>	The number of successful incremental updates since the initial publish operation or last full refresh.
<b>Publishing Status</b>	Indicates whether the last publishing event succeeded or failed.
<b>Event Number</b>	Unique number generated internally for each publishing operation.

## 14.3 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 “[Content delivery properties](#)” on page 360.  
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](#)” on page 361.
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](#)” on page 366.



**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” on page 367.
8. Click **OK** to save the content delivery configuration.

**Table 14-2: Content delivery properties**

Field	Description
<b>Info</b>	
<b>State</b>	Select <b>Active</b> to indicate using this content delivery configuration is active. The default state is Active.  Select <b>Inactive</b> to deactivate the configuration.
<b>Configuration Name</b>	Identifies the publishing configuration. The name appears in the list of existing configurations and the name of log files applying to the configuration.
<b>Publishing Folder</b>	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.
<b>Version</b>	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.
<b>Target Host Name</b>	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.
<b>Target Port</b>	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.

Field	Description
<b>Target UDP Port</b>	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.  The Target UDP Port option is available only in <i>IDSx</i> .
<b>Connection Type</b>	Can be <b>Secure</b> or <b>Non-secure</b> . This is the type of connection used for connections from the source host to the target host. The default is <b>Secure</b> .
<b>Target Root Directory</b>	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.  <i>CAUTION:</i> 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.

## 14.4 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 14-3: Advanced properties for content delivery**

Field	Description
<b>Property Export Settings</b>	
<b>Add properties as HTML Meta Tags</b>	If selected, the system inserts document properties into HTML content files as META tags on the target host.  If this setting changes after the initial publishing event for the configuration, republish using the Full Refresh option.

Field	Description
<b>Export Properties</b>	<p>If selected, the system exports a default set of properties for each published document.</p> <p>If this setting changes after the initial publishing event for the configuration, republish using the Full Refresh option.</p>
<b>Include contentless properties</b>	<p>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.</p> <p>By default, this option is not selected and is enabled only if <b>Export Properties</b> is also selected.</p>
<b>Include folder properties</b>	<p>If selected, folder properties are published to the website. This option is enabled only if <b>Include contentless properties</b> is also selected.</p>
<b>Additional Properties</b>	<p>Identifies additional properties to export to repository on target host. If <b>Export Properties</b> is selected, IDS exports a set of default properties for each published document.</p> <p>If this setting changes after initial publishing event for the configuration, republish using the Full Refresh option.</p> <p>Click <b>Select Attributes</b> to identify additional properties to export.</p>
<b>Property Table Name</b>	<p>The name to use when creating the database tables on the target host. Specify a table name if <b>Export Properties</b> is selected. The table name must not exceed 28 bytes.</p> <p>If this setting changes after initially publishing the configuration, republish the configuration using the Full Refresh option.</p>
<b>Content Selection Settings</b>	
<b>Formats</b>	<p>The content formats to publish. If specified, only documents with the listed formats are published. If unspecified, all formats are published.</p> <p>If this setting changes after publishing the configuration initially, republish the configuration using the Full Refresh option.</p>

Field	Description
<b>Effective Label</b>	<p>This field is used in conjunction with the <code>a_effective_label</code> document property to filter documents for publication. If Effective Label is specified, only documents with a matching <code>a_effective_label</code> value are examined as possible candidates for publication. If unspecified, all documents are examined as possible candidates.</p> <p>If this setting changes after initially publishing the configuration, you must republish the configuration using the Full Refresh option.</p>
<b>Miscellaneous Settings</b>	
<b>Export Directory</b>	<p>The name of the local directory on the Documentum CM Server host where documents are placed after they are exported from the repository.</p> <p>The default is a subdirectory of <code>\$DOCUMENTUM/share/temp</code>. When executing a publishing operation, the directory <code>\$DOCUMENTUM/share/temp/web_publish</code> is created.</p> <p>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 Documentum CM Server host is limited to 255 characters. There is no length limitation on Linux.</p>
<b>Ingest Directory</b>	<p>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 <code>\$DOCUMENTUM/share/temp</code>. You can choose a different directory by clicking <b>Select Directory</b>.</p>
<b>Trace Level</b>	<p>Defines a tracing level for IDS operations. The trace levels correspond to the trace levels available using the Trace API methods. The default value is 0.</p>
<b>Global Publishing Enabled</b>	<p>Enables the global publishing feature of Web Publisher. Replaces the <code>global_publishing</code> extra argument that was added manually to the content delivery configuration in prior versions.</p>

Field	Description
<b>Website Locale</b>	<p>Web Publisher only. Replaces the global_locales extra argument that was added manually to the content delivery configuration in prior versions.</p> <p>Select a locale from the drop-down list. If using Web Publisher and a document exists in more than one translation in the publishing folder, the locale code indicates which translation to publish and also points to the Web Publisher rules that define the second and subsequent choices of translation to publish.</p> <p>The drop-down list contains choices only when you are using Web Publisher and the publishing folder is configured for multilingual use.</p> <p>If you do not use Web Publisher or if your publishing folder is not configured for multilingual publishing, the drop-down list does not appear.</p>
<b>Web Server URL Prefix</b>	<p>This is the URL to the target root directory and is required if using Web Publisher.</p> <p>For example, if the target root directory is d:\inetpub\wwwroot\webcache and the website host is on a computer <i>host_name</i>, set the Web Server URL Prefix to http://<i>host_name</i>/webcache.</p> <p>Web Server URL Prefix is not applicable to replication targets.</p>
<b>Synchronization Settings</b>	
<b>Transfer is to live website</b>	<p>If selected, Interactive Delivery Services attempts to minimize user interruptions during publishing. Leave cleared if users do not have access to the site during publishing operations.</p> <p>If this setting changes after initial publication, republish the configuration using the Full Refresh option.</p>

Field	Description
<b>Online Synchronization Directory</b>	<p>The directory on the target host to be used as temporary storage for the backup copy of the Interactive Delivery Services repository during online updates. This must be specified if <b>Transfer is to live website</b> is selected.</p> <p>If this setting changes after you publish the configuration initially, republish the configuration using the Full Refresh option.</p>
<b>Pre-Synch Script on Target</b>	<p>The name of a script, located in the target host's product/bin directory, to run before publishing takes place. If online synchronization is enabled, the script runs before online synchronization occurs. There is a 48-character limit for information typed into this field.</p>
<b>Post-Synch Script on Target</b>	<p>The name of a script located in the target host's product/bin directory to be run after publishing occurs. If online synchronization is enabled, the script runs after online synchronization takes place. There is a 48-character limit for information typed into this field.</p>
<b>Ingest Settings</b>	
<b>Ingest</b>	<p>Select this option if you want to ingest content from the target to the repository.</p>
<b>Target Ingest Directory</b>	<p>Enter the directory path of the target from where the content will be ingested.</p>
<b>Transfer Authentication Settings</b>	
<b>Enable system authentication on target</b>	<p>Select to require a transfer username and password for authentication. Not selected means the transfer username and password are not required for authentication before a data transfer occurs.</p>
<b>User Name</b>	<p>Identifies the user whose account will be used by the transfer agent to connect to the target host.</p>
<b>Password</b>	<p>The password for the user specified in <b>User Name</b>.</p>
<b>Confirm Password</b>	<p>Enter the password again for confirmation.</p>
<b>Domain</b>	<p>Identifies the domain of the user specified in <b>User Name</b>.</p>

## 14.5 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 14-4: Content delivery replication properties**

Field	Description
<b>Replication Target Host Settings</b>	
<b>State</b>	You can select one of the following states: <ul style="list-style-type: none"><li>• <b>Active in-transaction:</b>Select this option if you want a replication target to participate in a transactional replication. This is the default value.</li><li>• <b>Active not-in-transaction:</b>Select this option if you want the replication target to participate in a non transactional replication.</li><li>• <b>Inactive:</b> Select this option if you want a replication target to go for system maintenance or out of commission.</li></ul>
<b>Target Host Name</b>	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.
<b>Target Port</b>	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.
<b>Target UDP Port</b>	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.
<b>Connection Type</b>	May be <b>Secure</b> or <b>Non-secure</b> . This is the type of connection used for connections from the source host to the target host. The default is <b>Secure</b> .

Field	Description
<b>Target Root Directory</b>	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.
<b>Export Properties</b>	You can select this check box to export properties to the replication target.
<b>Property Table Name</b>	Type the target host property table name, which is required if you selected <b>Export Properties</b> .
<b>Ingest</b>	Select this option if you want to ingest content from the replication target to the repository.
<b>Target Ingest Directory</b>	Enter the directory path of the source where the content will be stored.
<b>Transfer Authentication Settings</b>	
<b>User Name</b>	Enter the user name for the data transfer.
<b>Password</b>	Enter the password for the data transfer.
<b>Domain</b>	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.
<b>addReplicationTarget</b>	Adds multiple replication targets.

## 14.6 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 14-5: Extra arguments**

Key	Description	Default value(s)
use_docbase_formats	Determines whether the default file format extensions set in the repository are used when files are published.  FALSE overrides the default file format extensions set in the repository. TRUE or no setting uses the extensions set in the repository format objects.	TRUE
use_text_file_extensions	When set to TRUE, text files that do not have a .txt extension in the object name are published with the .txt extension. For example, if a text file MyFile is published and the parameter is set to TRUE, the file is published as MyFile.txt. If the parameter is set to FALSE, the default value, the file is published as MyFile.	FALSE
agent_connection_timeout	The timeout interval in seconds for the IDS publish method's connection to the target host. For example, to wait 90 seconds:  <code>agent_connection_timeout=90</code>  If the publishing operation takes longer, Documentum Administrator displays an error message and the publishing log files record that the publishing operation failed.	120
connect_thread_timeout	The timeout interval in seconds for the end-to-end tester's connection to the target host. For example, to wait 90 seconds:  <code>connect_thread_timeout=90</code>	30
lock_sleep_interval	The number of seconds for which IDS waits for a webc lock object to be unlocked. For example, to wait 90 seconds:  <code>lock_sleep_interval=90</code>	10

Key	Description	Default value(s)
lock_retry_count	<p>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.</p> <p>Since the default lock_sleep_interval value is 10 seconds, IDS retries for a total of 300 seconds (5 minutes) by default.</p>	30
disable_dctm_tag	Whether you want the Documentum META tag to appear when you use META tag merging.	TRUE
trace_passwords	Whether passwords appear in debug tracing output. FALSE causes passwords to be omitted from debug tracing output. TRUE causes passwords to be included in debug tracing output.	FALSE
error_threshold	The number of errors allowable on the source side during a single full-refresh, incremental, or force-refresh publishing operation.	0
max_cached_ssl_sockets	The number of cached SLL sockets between source and all targets that are retained for reuse. Does not restrict the maximum number of SLL sockets that can be open at one time. Used only in the scs_admin_config object in the IDS Administration sub-node.	30
publish_contentless_documents	<p>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.</p> <p> <b>Note:</b> This option can also be selected on the Advanced tab of the content delivery configuration.</p>	FALSE

Key	Description	Default value(s)
publish_folder_properties	Whether folder properties can be published. TRUE causes folder properties to be published. FALSE causes folder properties not to be published. If set to TRUE, requires that publish_contentless_documents is also set to TRUE.   <b>Note:</b> This option can also be selected on the Advanced tab of the content delivery configuration.	FALSE
compression	Whether file compression is enabled. TRUE causes files to be compressed. FALSE disables file compression.	TRUE
min_size_worth_compressing	The threshold in bytes beneath which compression of a particular file does not yield performance gains	5000
max_entries_per_zipfile	The number of files whose size is lesser than min_size_worth_compressing that are collected in a ZIP file for transfer to the target host.	128
extensions_to_compress	The file types to compress, by file extension.	html, jhtml, shtml, phtml, xhtml, htm, jht, sht, asp, jsp, xml, css, txt
publish_source_version_labels	When set to TRUE, all values of the r_version_label attribute are published to the repeating attribute table.	FALSE
mssql_store_varchar	Microsoft SQL Server database only. When set to TRUE, string attributes are stored in the source catalog database and target database as varchar rather than nvarchar.  When set to true, you cannot publish multibyte data.	FALSE

Key	Description	Default value(s)
store_log	<p>Whether to store log files in the repository. Valid values are:</p> <ul style="list-style-type: none"> <li>• TRUE: The logs are stored in the repository.</li> <li>• FALSE: The logs are not stored in the repository.</li> </ul> <p>The log is not stored in the repository for a single-item publishing operation when method_trace_level is set to 0.</p>	TRUE
store_log_file	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.	
method_trace_level	<p>The level of tracing output. 0 is the lowest level of tracing and 10 is the highest level of tracing.</p> <p> <b>Note:</b> To get LDAPSsync debug information, use method_trace_level 8. To get verbose debug information, use method_trace_level 10.</p>	0
export_threshold_count	Indicates the number of items the export operation exports at one time.	100

Key	Description	Default value(s)
use_format_extensions	<p>Use with format key to check for valid format extensions.</p> <p>If use_format_extensions is set to FALSE, files are published with the format extensions defined in the repository for the format.</p> <p>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.</p> <p>If use_format_extensions is set to TRUE and a particular extension is <i>not</i> defined as valid for a particular format, files of that format with that extension are published with the format extensions defined in the repository for the format.</p>	FALSE
format	<p>Use with use_format_extensions key. Takes the format:</p> <p>format.format_name=semicolon-separated_extensions</p>	
force_serialized	When set to TRUE, single-item publishes are performed serially rather than in parallel.	FALSE
sourceAttrsOnly	<p>By default, on each publish IDS creates a properties.xml file, which contains <i>all</i> the attributes of the objects published. If sourceAttrsOnly is set, IDS writes only the default attributes and any additional attributes that are published to the XML file.</p> <ul style="list-style-type: none"> <li>• r_object_id</li> <li>• r_modified_date</li> <li>• object_name</li> <li>• i_chronicle_id</li> <li>• r_version_label</li> <li>• content_id</li> <li>• i_full_format</li> <li>• r_folder_path</li> </ul>	FALSE

Key	Description	Default value(s)
additional_metatag_file_exts	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:  additional_metatag_extensions=asp;jsp;jht;sht	No default value.
export_relations	When set to TRUE and attributes are published, relation objects (dm_relation objects) are published to a database table on the target.	FALSE
clean_repeating_table_no_attributes	Deprecated.	
export_media_properties	When set to true, attributes of the dmr_content object and dm_format object are exported and published to the target.	FALSE
additional_media_properties	When export_media_properties is set to true, used to specify additional attributes of dmr_content and dm_format objects to be published. The format is a semicolon-separated list:  additional_media_properties=<type1.attribute1;type2.attribute2>  For example:  additional_media_properties=dmr_content.x_range;dmr_content.z_range	FALSE
exclude_folders	A semicolon-separated list of absolute repository paths, indicates the folders to be excluded from a publishing operation. When set, content files and attributes from folders indicated are not published. For example:  exclude_folders=/acme.com/images;/acme.com/subdir	
pre_webroot_switch_script	A script to be run before online synchronization takes place. <i>OpenText Documentum Interactive Delivery Services User Guide</i> provides the detailed information.	
post_webroot_switch_script	A script to be run after online synchronization takes place. <i>OpenText Documentum Interactive Delivery Services User Guide</i> provides the detailed information.	

Key	Description	Default value(s)
full_refresh_backup	When set to TRUE, the content files and database tables on the target host are backed up before the synchronization phase in a full-refresh publishing operation.	FALSE
exclude_formats	Takes a semicolon-separated list of format extensions and excludes content files with those extensions from publishing. For example to exclude .xml and .wml files: <code>exclude_formats=xml;wml</code>	Not set
check_valid_filename	If this parameter is set to TRUE, then the filename is checked for Windows illegal characters. Illegal characters are replaced as specified by the filename_replace_char parameter.  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.	TRUE (Windows only); FALSE for all other operating systems
filename_replace_char	Windows only. Used in conjunction with check_valid_filename. Defines the character to use to replace invalid characters in file names on Windows. For example: <code>filename_replace_char=_</code>	_ (underscore)
sync_on_zero_updates	When set to TRUE, database updates are made and pre- and post-synch scripts are run even if there is no new data to publish from the repository.	FALSE
transform_type	Used with Web Publisher Page Builder only.  Determines whether links in HTML pages are resolved at publication time to absolute or relative paths. Valid values are absolute and relative.	absolute
recovery_publish_retry_count	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.	

Key	Description	Default value(s)
set_tcp_delay	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.	FALSE
ingest_workflow	Used with Content Delivery web service only. Specifies a custom workflow to be used with the ingest operation. <i>OpenText Documentum Content Management - Enterprise Content Services Reference Guide (EDCPKSV250400-ARC)</i> provides the information about this web service.   <b>Note:</b> 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)
wan_acceleration_policy	<p>This parameter defines the policy used for accelerated data transfer.</p> <ul style="list-style-type: none"> <li>• 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.</li> <li>• 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.</li> <li>• 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.</li> </ul>	A
min_file_transfer_rate	This is the minimum file transfer rate	0 Mbps
max_file_transfer_rate	This is the maximum file transfer rate	1000 Mbps
wan_acceleration_log_details	The file transfer process status are captured in the content delivery log files	FALSE

Key	Description	Default value(s)
wan_acceleration_file_checks um	<p>This parameter is used to resume file transfer when there is a failure.</p> <ul style="list-style-type: none"> <li>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.</li> <li>FULL_CHECKSUM: When set to this value, checks for the checksum of both files. If it matches, then transfer does not take place</li> <li>SPARSE_CHECKSUM: When set to this value, checks for the sparse checksum of both files. If it matches, then transfer does not take place</li> <li>OFF: When set to this value, the file gets replaced</li> </ul> <p>When set to OFF, the rate of file transfer is high.</p>	OFF
decision_commit_rollback	<p>This parameter is used to set the threshold value for transaction capability. For example, if there are 10 replication targets, and if the DCR value reads as:</p> <pre>decision_commit_rollback 6</pre> <p>implies that if replication operation succeeds on a minimum of 6 replication targets, then a decision is taken to commit (File System and RDBMS) the changes performed by the replication operation.</p> <p>If the <i>number_of_failures</i> value is greater than the <i>decision_commit_rollback</i> value, a rollback is initiated on the replication targets.</p> <p>The value assigned to this attribute must be a positive integer.</p>	NA
tc_file_count	<p>The transaction capability is based on <i>tc_file_size</i> and <i>tc_file_count</i>.</p> <p>When the number of files replicated exceeds <i>tc_file_count</i>, transaction capability feature is disabled.</p> <p>The value assigned to this attribute must be a positive integer.</p>	500

Key	Description	Default value(s)
tc_file_size	<p>The transaction capability is based on <i>tc_file_size</i> and <i>tc_file_count</i>.</p> <p>When the size of the files replicated exceeds <i>tc_file_size</i>, transaction capability feature is disabled. The units is specified in MB.</p> <p>The value assigned to this attribute must be a positive integer.</p>	100 MB
use_replication_time	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.	TRUE
use_repository_time	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).	TRUE
lock_exitifbusy_flag	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.	TRUE

Key	Description	Default value(s)
auto_replication	Replication can be invoked automatically after a publishing operation by setting the extra argument auto_replication to TRUE in Documentum Administrator.   <b>Note:</b> 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.	TRUE
full_refresh.Transactional_repliCation	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.	FALSE
post_replication_script_on_staging_target	Use this script to perform any arbitrary action on the staging target after replication is complete on all replication targets.	No default value.

## 14.7 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](#)” on page 381 provides instructions on how to deactivate a publishing configuration.

### To delete a content delivery configuration:

1. Connect to the repository from which you are publishing.
2. Navigate to **Administration > Content Delivery > IDS Configurations** to access the Interactive Delivery Services Configuration list page.
3. Select the content delivery configuration to delete and then select **File > Delete**.  
The system displays a delete confirmation page.

4. Click **OK** or **Cancel**.
  - Click **OK** to delete the content delivery configuration.
  - Click **Cancel** to return to the Interactive Delivery Services Configuration list page without deleting the configuration.

## 14.8 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.

## 14.9 Duplicating a content delivery configuration

Create a new content delivery configuration by duplicating and then modifying a content delivery configuration that is thoroughly tested and successfully used in production. The IDS Configuration Template stores default values that you can use to create new content delivery configurations.

### To duplicate a content delivery configuration:

1. Connect to the repository from which you are publishing.
2. Navigate to **Administration > Content Delivery > IDS Configurations**.  
The Interactive Delivery Services Configuration list page appears.
3. Select the content delivery configuration to duplicate and then select **File > Save as**.

The **New Content Delivery Configuration - Info** page for the new content delivery configuration appears. The object name of the configuration defaults to:

`Copy [1] of configuration_name`

where *configuration\_name* is the name of the original configuration.

4. Modify fields that need to be changed on the New Content Delivery Configuration - Info, New Content Delivery Configuration- Advanced, New Content Delivery Configuration - Replication, and New Content Delivery Configuration - Extra Arguments pages.  
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.

## 14.10 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.

## 14.11 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 option forces a full-refresh publish.
  - **Update property schema**: Select to update the database tables with schema changes, but without republishing all content files and metadata.
  - **Launch the process asynchronously**: Select to refresh the screen before publishing is complete.  
If you do not select Launch process asynchronously, the screen does not refresh before publishing is completed and your browser may time out.
  - **Trace Level**: Select a trace level.
5. Click **OK**.  
If you selected **Refresh entire site** or **Recreate property schema**, a warning message appears.
6. Click **OK**.

The publishing job runs and the results are displayed. Note that it may take several minutes for the publishing log to be available from Documentum Administrator.

#### To replicate from a content delivery configuration

1. Connect to the repository from which you are replicating.
2. Navigate to **Administration > Content Delivery > IDS Configurations**.  
The **Interactive Delivery Services Configuration** list page appears.
3. Select the correct content delivery configuration and then select **Tools > Replicate**.  
The **Content Delivery Configuration Replicate** page appears.
4. Select a trace level.
5. Click **OK**.

The replication job runs and the results are displayed in the **Content Delivery Configuration Replicate Result** page. In this page, you can also click the link available to view the logs. Note that it may take several minutes for the Replication log to be available from Documentum Administrator.

#### To ingest from a content delivery configuration

1. Connect to the repository from which you are replicating.
  2. Navigate to **Administration > Content Delivery > IDS Configurations**.  
The **Interactive Delivery Services Configuration** list page appears.
  3. Select the correct content delivery configuration and then select **Tools > Ingest** or right-click on the content delivery configuration and then select **Ingest**.  
The **Content Delivery Configuration Ingestion** page appears.
  4. Select a trace level.
  5. Click **OK**.
- The **Content Delivery Configuration Ingestion Result** page appears. In this page, you can also click the link available to view the logs. Note that it may take several minutes for the Ingestion log to be available from Documentum Administrator.

## 14.12 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. *OpenText Documentum Interactive Delivery Services User Guide* and *OpenText Documentum Interactive Delivery Services Accelerated User Guide* documentation provides more information.

## 14.13 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.

### 14.13.1 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**.

## 14.13.2 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.

## 14.14 Effective labels

Use *effective labels* to enable IDS to determine which documents to publish based on effective and expiration dates.

The effective label specified in a content delivery configuration allows IDS to determine when to publish a particular document and when to delete it from the website. IDS does this by examining the repeating properties `a_effective_label`, `a_effective_date`, and `a_expiration_date`, which are properties of the `dm_sysobject` type. These properties are inherited by all subtypes of `dm_sysobject`.

Each `a_effective_label` corresponds to a matching `a_effective_date` and `a_expiration_date`. Because these are repeating properties, you can specify multiple effective labels, effective dates, and expiration dates for each document. IDS looks for the effective and expiration dates matching a particular effective label, and uses the dates to determine when to publish a document and when to withdraw the document from the website.

For example, a document might have the effective label, effective date, and expiration date properties set as follows:

**Table 14-6: Using effective labels**

<code>a_effective_label</code>	<code>a_effective_date</code>	<code>a_expiration_date</code>
DRAFT	03/05/08	03/15/08
REVIEW	03/16/08	03/26/08
COMMENT	03/27/08	04/10/08
APPROVED	04/10/08	04/10/09

Setting the document's effective label to REVIEW means the document will be published on March 16, 2008 and removed from the website on March 26, 2008.

Setting the effective label to APPROVED means the document will be published on April 10, 2008 and withdrawn on April 10, 2009.

Documents whose effective label does not match the effective label set in the content delivery configuration are published regardless of the values set for effective date and expiration date.

# Chapter 15

## Indexing management

### 15.1 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 Documentum CM Server. The index agent prepares documents for indexing and Documentum xPlore creates indexes and responds to queries from Documentum CM Server. *OpenText 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. *OpenText Documentum xPlore Administration Guide* provides information on editing the properties of the index agent configuration object and other full-text configuration objects.

### 15.2 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 Documentum CM Server.

### 15.3 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 Accelerated Content Services server is started. You must enable the index agent before starting it. [“Enabling index agents” on page 389](#) 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 Documentum CM Server is in a *projected to dormant* state, then starting or stopping the index agent works correctly. However, if the Documentum CM 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.

## 15.4 Disabling index agents

An index agent that is disabled cannot be started and is not started automatically when its Accelerated Content Services 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](#)” on page 389.

#### 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.

## 15.5 Enabling index agents

An index agent that is disabled cannot be started (if it is stopped) and is not started automatically when its Accelerated Content Services server is started. 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.

## 15.6 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.

## 15.7 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.

## 15.8 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. *OpenText Documentum xPlore Administration Guide* provides instructions about resubmitting objects for indexing.

### 15.8.1 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**.

### 15.8.2 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**.

### 15.8.3 Removing 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. Select **Tools > Remove Queue Items by Status** and then select the correct status.

## 15.8.4 Removing queue items

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, select the queue items, and then select **Tools > Remove queue items**.

## 15.8.5 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 and select the object.
3. Select **View > Associated Index Queue Items**. The queue items are displayed for the selected index queue.
4. If the repository's indexing system is installed in a high-availability configuration, optionally click the links for each index queue.

## 15.8.6 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, select the object and then select **File > New > Create queue item**.

## Chapter 16

# Transformation Services management

## 16.1 Transformation Services

Transformation Services version 7.3 and later encapsulates the functionality of all transformation components that are OpenText™ Documentum™ Content Management Transformation Services - Documents, OpenText™ Documentum™ Content Management Transformation Services - Media, OpenText™ Documentum™ Content Management Transformation Services - Audio/Video, and XML Transformation Services and requires just one installation, rather than multiple installation processes for multiple Transformation Services components.

Transformation Services 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 Transformation Services instances. All Transformation Services instances polling the repository are displayed in the **Content Transformation Services** node in Documentum Administrator.

## 16.2 Changing the Transformation Services user

This feature allows you to change the user name that a Transformation Services 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 Transformation Services user, the user's password is required.

### To change the user name used by the Transformation Services instance:

1. Connect to the repository where the Transformation Services instance is located.
2. Click the **Administration > Content Transformation Services** node.
3. Click the **CTS Instances** node or link.
4. Select the Transformation Services 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**.

## 16.3 Configuring a Transformation Services instance

This feature allows you to update some of the Transformation Services configuration parameters.

### 16.3.1 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 Transformation Services instance:**

1. Connect to the repository where the Transformation Services instance is located.
2. Click the **Administration > Content Transformation Services** node.
3. Click the **CTS Instances** node or link.
4. Select the Transformation Services instance that you want to configure from the list of available instances.
5. Click **Tools > Content Transformation Services > Configure > Service**.
6. On the **Configure CTS instance** page, type a number to represent the polling interval in the **Polling interval** field.  
The minimum interval time is 2 seconds.
7. Click **OK**.

### 16.3.2 Changing the logging level

The logging level value controls how much information will be recorded in the Transformation Services 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 Transformation Services 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 Transformation Services instance:**

1. Connect to the repository where the Transformation Services instance is located.
2. Click the **Administration > Content Transformation Services** node.
3. Click the **CTS Instances** node or link.
4. Select the Transformation Services instance that you want to configure from the list of available instances.
5. Click **Tools > Content Transformation Services > Configure > Service**.
6. On the **Configure CTS instance** page, select a value for the new logging level from the **Logging Level** drop down.
7. Click **OK**.

### 16.3.3 Changing the System Operator

The System Operator is the name of the user that receives messages from an instance of Transformation Services.

**To change the operator used by an instance of Transformation Services:**

1. Connect to the repository where the Transformation Services instance is located.
2. Click the **Administration > Content Transformation Services** node.
3. Click the **CTS Instances** node or link.
4. Select the Transformation Services instance that you want to configure from the list of available instances.
5. Click **Tools > Content Transformation Services > Configure > Service**.
6. On the **Configure CTS instance** page, select a user name from the **Operator** drop down.
7. Click **OK**.

### 16.3.4 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 Transformation Services product.

**To change the notification setting for an instance of Transformation Services:**

1. Connect to the repository where the Transformation Services instance is located.
2. Click the **Administration > Content Transformation Services** node.
3. Click the **CTS Instances** node or link.
4. Select the Transformation Services instance that you want to configure from the list of available instances.
5. Click **Tools > Content Transformation Services > Configure > Service**.
6. On the **Configure CTS instance** page, select either YES or NO in the **Send Notification** drop down.
7. Click **OK**.

### 16.3.5 Changing the maximum number of queue items

The value for a maximum number of queue items controls how many items the Transformation Services 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 Transformation Services instance:**

1. Connect to the repository where the Transformation Services instance is located.
2. Click the **Administration > Content Transformation Services** node.
3. Click the **CTS Instances** node or link.
4. Select the Transformation Services instance that you want to configure from the list of available instances.
5. Click **Tools > Content Transformation Services > Configure > Service**.
6. On the **Configure CTS instance** page, type a number to represent the maximum number of queue items for the Transformation Services instance in the **Max Queue Items to Sign Off** field.
7. Click **OK**.

### 16.3.6 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 Transformation Services instance is located.
2. Click the **Administration > Content Transformation Services** node.
3. Click the **CTS Instances** node or link.
4. Select the Transformation Services instance that you want to configure from the list of available instances.
5. Click **Tools > Content Transformation Services > Configure > Service**.
6. On the **Configure CTS instance** page, type 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**.

## 16.4 Viewing a Transformation Services log file

Log files are created for each Transformation Services product and component. The contents and detail level of each log file depend on the log file setting you have chosen for the Transformation Services instance (see “[Changing the logging level](#)” on page 394).

The log files screen lists available log files on the Transformation Services host and allows you to choose a log file for viewing. The selected log file opens in a new window.

**To view a Transformation Services log file:**

1. Connect to the repository where the Transformation Services instance is located.
2. Click the **Administration > Content Transformation Services** node.
3. Click the **CTS Instances** node or link.
4. Select the Transformation Services 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 check box and click **OK**.

The selected log file opens in a new window.

## 16.5 Viewing details of a Transformation Services instance

The Transformation Services 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 Transformation Services 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 Transformation Services 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 Transformation Services instance:

1. Connect to the repository where the Transformation Services instance is located.
2. Click the **Administration > Content Transformation Services** node.
3. Click the **CTS Instances** node or link.
4. Select the Transformation Services instance that you want to view details for and select **View > Properties**.
5. The details for the selected Transformation Services instance are displayed.

When you are finished viewing the details, click **Close**.

## 16.6 Controlling your Transformation Services instance

The Transformation Services instance details screen also allows you to select a particular Transformation Services product and either start, stop, or refresh it.

You can also start, stop, and refresh an entire Transformation Services instance through easily accessible menu items.

### 16.6.1 Stopping the Transformation Services service

You can stop a Transformation Services service when the instance is currently running. Any items that are currently in the processing queue are removed.

#### To stop a Transformation Services instance:

1. Connect to the repository where the Transformation Services instance is located.
  2. Click the **Administration > Content Transformation Services** node.
  3. Click the **CTS Instances** node or link.
  4. Select the Transformation Services instance that you want to stop from the list of available instances.
    - Click **Tools > Content Transformation Services > Stop**.
- OR
- Select the Transformation Services instance that you want to stop from the list of available instances and select **View > Properties > Info**.
- On the **CTS Instance Details** page, click **Stop**.

### 16.6.2 Starting the Transformation Services service

You can start a Transformation Services service when the instance is currently stopped. The refreshed date and time is shown when the page is reloaded.

#### To start a Transformation Services instance:

1. Connect to the repository where the Transformation Services instance is located.
  2. Click the **Administration > Content Transformation Services** node.
  3. Click the **CTS Instances** node or link.
  4. Select the Transformation Services instance that you want to start from the list of available instances.
    - Click **Tools > Content Transformation Services > Start**.
- OR

- Select the Transformation Services instance that you want to start from the list of available instances and select **View > Properties**.

On the **CTS Instance Details** screen, click **Start**.

### 16.6.3 Refreshing the Transformation Services service

Refreshing a Transformation Services instance forces it to re-initialize its configuration files without stopping and starting the service. This is typically used after updating some of the Transformation Services configuration files. The Transformation Services instance activation date and time is refreshed to show the correct date and time of activation. The Transformation Services queue is unaffected by a refresh.

#### To refresh a Transformation Services instance:

1. Connect to the repository where the Transformation Services instance is located.
  2. Click the **Administration > Content Transformation Services** node.
  3. Click the **CTS Instances** node or link.
  4. Select the Transformation Services instance that you want to refresh from the list of available instances.
    - Click **Tools > Content Transformation Services > Refresh**.  
OR
    - Select the Transformation Services 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.

## 16.7 Transformation Services reporting

Transformation Services reporting allows you to monitor your Transformation Services 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 Transformation Services 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 Transformation Services performance on your repository.

To enable or disable Transformation Services reporting, refer to the Administration Guide for your Transformation Services product.

## 16.7.1 Configuring Transformation Services reporting

Report configuration is performed on a repository. This means that all Transformation Services instances that are configured for the current repository will follow this configuration.

### To configure Transformation Services reporting:

1. Connect to the repository where one or more Transformation Services 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.

## 16.7.2 Viewing archived Transformation Services reporting data

Archived Transformation Services reporting data is viewable through Documentum Administrator. When a user enters start and end times, Documentum Administrator 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 Transformation Services reporting data. Administrator users can view all Transformation Services reporting data.

### To view archived Transformation Services reporting data:

1. Login to the repository you want to view data for, using Documentum Administrator.
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.

## 16.8 Viewing transformation request in queue

When you select a document for transformation with a target format, the request goes to a queue where Transformation Services processes it. The Transformation screen displays the queue.

Click **Administration > Content Transformation Services > Transformation**, to view the Transformation screen. You can track the transformation requests listed in the queue.

- When the queue item is signed off, it is updated in the **Sign-off User** field in the Transformation screen.
- When the request is processed and completed as passed or failed, the queue item is deleted.

## 16.9 Transformation Services profiles

The Profiles screen lists all transformation profiles installed in the repository. The Content Transformation Services Profile Editor allows you to create and modify transformation profiles. *OpenText Documentum Content Management - Transformation Services Administration Guide (EDCCT250400-AGD)* provides more information to modify Transformation Services profiles. *OpenText Documentum Content Management - Transformation Services Development Guide (EDCCT250400-PGD)* provides more information to develop custom Transformation Services plug-ins, including transformation profiles and command line files.

### 16.9.1 Building new transformation profiles

The Content Transformation Services Profiles Editor allows you to create new transformations using the transformation profiles that are installed in the repository by the Content Transformation products. You can build new transformation profiles using an existing profile as a template, chaining multiple profiles together, or sequencing multiple profiles. All transformation profiles are created as `dm_media_profile` objects in the repository. The Transformation Wizard and the Profiles Editor retrieve all `dm_media_profile` objects from the repository when you invoke these objects.

### 16.9.1.1 Using a transformation profile to create a new transformation profile

You can use an existing transformation profile as a template to create a new transformation profile. The new profile can perform a similar transformation with few different parameters.

1. Click **Administration > Content Transformation Services > Profiles**.
2. Select a transformation profile that you want to use as a template for the new profile.
3. Click **Tools > Build Profile > From Existing**.
4. Enter a new profile name, label, and description.
5. Select the products that can use this profile.
6. Enter a location in the repository where the profile must be saved. The Profiles folder (`//System/Media Server/Profiles`) is specified, by default.
7. Select **System**, to save the profile as a system profile. System profiles are not visible to users in the Transformation wizard, but may be used internally by Transformation Services products.
8. Click **Next**.
9. Click **Add**, to add another Source and Target format pairing for the new profile. These are the source file formats that the profile will accept for transformation and the target formats for transforming the files. Click **OK**.
10. Select the pairing and click **Remove** to remove a Source and Target format pairing from the new profile.
11. Click **Next**.
12. To configure the profile parameters select a parameter and click **Configure**.
13. Click **OK**.
14. Click **Next**.
15. Click **Finish**.

### 16.9.1.2 Chaining transformation profiles

A chained transformation profile contains multiple inner profiles that are invoked in stages. Transformations occur one at a time, and the result of one transformation is required for the next transformation. The result of a chained profile is one output file.

**To chain multiple transformation profiles:**

1. Click **Administration > Content Transformation Services > Profiles**.
2. Select one or more transformation profiles from the Profiles list to chain together.
3. Click **Tools > Build Profile > Chain**.
4. Enter a new profile name, label, and description.
5. Enter a location in the repository where the profile must be saved. The Profiles folder (//System/Media Server/Profiles) is selected, by default.
6. Select **System**, to save the profile as a system profile. System profiles are not visible to users in the Transformation wizard, but may be used internally by Transformation Services products.
7. Click **Next**.
8. Select the existing profiles to chain together and create the new profile. If you have selected any profiles before launching the profile editor, then these profiles are included in the **Selected Profiles** list.

Select a profile in the **Selected Profiles** list and use the arrow keys to change the order in which the inner profiles are performed within the new profile.

9. Click **Next**.
10. Select a profile and click **Configure**.
11. Select an output format for the profile. This output file is used by the next profile in the chain, if applicable.
12. Click **OK**.
13. Click **Next**.
14. Click **Add**, to add another Source and Target format pairing for the new profile. Click **OK**.
15. Select the pairing and click **Remove** to remove a Source and Target format pairing from the new profile.
16. Click **Next**.
17. To configure the profile parameters select a parameter and click **Configure**.
18. Click **OK**.

19. Click **Next**.
20. Click **Finish**.

### 16.9.1.3 Building a sequenced transformation profile

Sequenced profiles specify a list of profiles that are executed in parallel. For each inner profile in the profile sequence, you can specify whether the next profile should wait for the successful completion of the previous task before it is executed. If there is no specification, profiles are executed as soon as the task's threads are available to process them. Profiles in a sequenced transformation profile are built and processed in parallel.

1. Click **Administration > Content Transformation Services > Profiles**.
2. Select one or more transformation profiles from the Profiles list that you want to build.
3. Click **Tools > Build Profile > Parallel**.
4. Enter a new profile name, label, and description.
5. Enter a location in the repository where the profile must be saved. The Profiles folder (//System/Media Server/Profiles) is selected, by default.
6. Select **System**, to save the profile as a system profile. System profiles are not visible to users in the Transformation wizard, but may be used internally by Transformation Services products.
7. Click **Next**.
8. Select the existing profiles that you want to use to create the new profile. If you have selected any profiles before launching the profile editor, these profiles are included in the **Selected Profiles** list.  
Select a profile in the **Selected Profiles** list and use the arrow keys to change the order in which the inner profiles are performed within the new profile. If you want a profile wait for the preceding inner profile before performing the transformation.
9. Click **Next**.
10. Select a profile and click **Configure**.
11. Select an output format for the profile. The next profile in the chain uses this output file, if applicable
12. Select **Wait on completion** if the next profile in the chain must wait for this profile to finish its transformation before the next profile can begin, to use its output.
13. Click **OK**.
14. Click **Next**.

15. To add another Source and Target format pairing for the new profile, click **Add** in the Formats tab. The format pairing include the source file formats that the profile will accept for transformation and the target formats that the source files can transform to. Click **OK**.
16. To remove a Source and Target format pairing from the new profile, select the pairing and click **Remove**.
17. Click **Next**.
18. Select the profile and click **Configure** to modify the parameters for each profile in the sequenced profile.
19. Click **Next**.
20. Click **Finish**.

### 16.9.2 Editing transformation profiles

You can edit transformation profiles to customize their properties and parameters. You can edit the profiles and any custom profiles you have created.

1. Click **Administration > Content Transformation Services > Profiles**.
2. Select a transformation profile from the Profiles list.
3. Click **Tools > Edit Profile**.



**Note:** When you are editing a profile, it is checked out from the repository and is inaccessible to users. After you complete editing the profile, it is checked back in to the repository and versioned automatically.

# Chapter 17

## Content Intelligence Services

### 17.1 Overview

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 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*: This 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.

#### 17.1.1 Classic categorization in Webtop

Like in the previous OpenText Documentum CM 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.

### 17.1.2 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.

## 17.2 Configuring Content Intelligence Services in Documentum Administrator

### 17.2.1 Setting up Content Intelligence Services for classic categorization

Before you can use CIS for classic categorization, install and start the CIS server. *OpenText Documentum Content Management - Server and Server Extensions Installation Guide (EDCSY250400-IGD)* 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.

### 17.2.2 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:

[2001:0db8:0:0:0:1428:57ab]  
[2001:0db8:0:0:0:1428:57ab]: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.

### 17.2.3 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. Type the 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.

## 17.2.4 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:** Categories can be linked to other categories in other taxonomies. If any of the categories in a taxonomy includes links to categories in other taxonomies, all related taxonomies must be synchronized to avoid possible errors.

## 17.2.5 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:

- Depending on your use of the categorization functionality, proceed with one 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. Download the Content Intelligence Services archive file 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 guidelines for module deployment described in the *Documentum Composer* documentation.

## 17.3 Building taxonomies for classic categorization

### 17.3.1 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 object that serves as the root level of the hierarchy.

Taxonomies consist of three types of 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). *OpenText Documentum Content Intelligence Services Administration Guide* provides more information about importing taxonomies.

### 17.3.2 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.

### 17.3.3 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.

### 17.3.4 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 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`.

### 17.3.5 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.

### 17.3.6 Viewing taxonomies and categories using Documentum Administrator

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 17-1: Views for categories in Documentum Administrator**

<b>View</b>	<b>Description</b>
<b>Administration &gt; Content Intelligence &gt; My Categories</b>	Displays all categories at the same level as a flat list. This view provides direct access to the categories for which you are the owner so that you can review documents. You can view all documents assigned to the categories you own, or only documents pending approval.
<b>Administration &gt; Content Intelligence &gt; Taxonomies</b>	Displays categories in their proper hierarchical position. This view is the configuration and administration view for taxonomies and categories. Use this view to create and configure categories.
<b>Categories cabinet</b>	Displays the hierarchy of categories and the documents assigned to these categories. This view is the end user view of the categories.

### 17.3.7 Providing evidence

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. *OpenText 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.

### 17.3.8 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 17-2: Confidence values for evidence terms**

Confidence value (0 – 100)	Description
High (75)	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.
Medium (50)	A term with medium confidence is a good indicator that a document belongs to the category.

Confidence value (0 – 100)	Description
Low (15)	<p>A term with low confidence only suggests that the category might be appropriate.</p> <p>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 <i>and</i> other evidence of the same category in the document.</p>
Supporting	<p>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.</p>
Exclude	<p>If one of the evidence terms found in a document has this confidence level, then the document is not assigned to the category.</p> <p>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.</p>
Required	<p>These terms are must-have terms but they are not taken into account for the document score.</p> <p>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.</p>

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.

### 17.3.9 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. *OpenText Documentum Content Intelligence Services Administration Guide* provides information on how to define patterns.

### 17.3.10 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.

### 17.3.11 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. 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.

### 17.3.12 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. 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.

### 17.3.13 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.

### 17.3.14 Defining category classes using Documentum Administrator

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 information 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** check box. When the check box 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**.

### 17.3.15 Defining taxonomies using Documentum Administrator

Create a taxonomy object before creating the categories in the hierarchy. The taxonomy object sets some default values for the categories.

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 17-3: Taxonomy settings**

Field	Description
<b>Name</b>	The taxonomy name is mandatory and must be unique. Once set, it cannot be modified.  By default, the taxonomy name is the text that appears in the list of taxonomies. However, it is possible to display the taxonomy title instead of the taxonomy name.
<b>Title</b>	The title is not mandatory and it is not necessarily unique.

Field	Description
Description	The description is not mandatory.

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.

### 17.3.16 Defining categories using Documentum Administrator

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 17-4: Taxonomy settings**

Field	Description
<b>Name</b>	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.
<b>Title</b>	The title is not mandatory and it is not necessarily unique.

Field	Description
Description	The description is not mandatory.

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.
  - 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 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** check box. When the check box 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.

### 17.3.17 Defining property rules using Documentum Administrator

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 in the **Rules** column.  
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:](#)” on page 432, describes how to make custom object types available in the CIS component.
  7. To assign documents based on their attributes, select the **Properties** check box 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](#)” on page 432, 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 the date standards. “[Date formats for property rules](#)” on page 428 demonstrate a non-exhaustive list of possible date formats.

**Table 17-5: Date formats for property rules**

Date format	Example
mm/dd/yy	02/15/1990
mon dd yyyy	Feb 15 1990
mm/yy	02/90
dd/mm/yyyy	15/02/1990
yyyy/mm	1990/02
yy/mm/dd	90/02/15
yyyy-mm-dd	1990-02-15
dd-mon-yy	15-Feb-90
month yyyy	February 1990
month dd yy	February 15 90
month, yyyy	February, 1990
month dd, yyyy	February 15, 1990

Property rules on a date attribute do not take into account the time (hours, minutes, seconds).

- e. To add an additional condition, click the **Add Property** button and repeat steps b through d.

8. Click **OK** to return to the rules page.

### 17.3.18 Defining evidence terms using Documentum Administrator

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 information 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**.

### 17.3.19 Synchronizing taxonomies with CIS server using Documentum Administrator

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. *OpenText 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.

### 17.3.20 Making taxonomies available using Documentum Administrator

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**.

### 17.3.21 Setting permissions for Content Intelligence using Documentum Administrator

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`.
4. Navigate to **Administration > User Management > Roles**.
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**.

### 17.3.22 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.

### 17.3.23 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.

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 qualiferrules\_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>
```

### 17.3.24 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 tab, you can create a custom tab for their subtypes.

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.

### 17.3.25 Deleting category classes using Documentum Administrator

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.

### 17.3.26 Deleting taxonomies using Documentum Administrator

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.
3. Select **File > Delete**.  
A message page appears asking you to confirm that you want to delete the taxonomy.
4. Click **OK**.

## 17.4 Selecting and submitting the documents to analyze

### 17.4.1 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.

### 17.4.2 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.

### 17.4.3 Defining document sets using Documentum Administrator

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**.
2. Select **File > New > Document Set**.
3. In the **Properties** page, enter a name and description for the document set.
4. Configure the document set as described in “[Configuring a document set using Documentum Administrator](#)” on page 436.
5. Schedule it as described in “[Scheduling a document set using Documentum Administrator](#)” on page 438.
6. Synchronize it as described in “[Synchronizing a document set using Documentum Administrator](#)” on page 439.

### 17.4.4 Configuring a document set using Documentum Administrator

**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 17-6: Document Set Builder settings**

Field	Description
<b>Look in</b>	To include documents from a specific folder, click <b>Select</b> next to <b>Look in:</b> and navigate to the folder containing the documents to process.

Field	Description
<b>Type</b>	<p>For classic categorization, to specify the object type of the documents selected for processing, click <b>Select</b> next to <b>Type:</b> and select the object type.</p> <p>In an xCP environment, the document set is automatically configured to process an object model.</p> <p>CIS processes the documents corresponding to the selected object type, including all the documents whose type is inherited from the selected object type.</p>
<b>Properties</b>	<p>Make sure <b>Properties</b> is already selected to assign documents based on their attributes. Enter the criteria used to select documents.</p> <p>For each rule, select an attribute, an operator and enter a value to test against.</p> <p>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.</p>
<b>Add Property</b>	To add another rule, click <b>Add Property</b> .

5. 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.

## 17.4.5 Viewing the documents in a document set using Documentum Administrator

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.

## 17.4.6 Scheduling a document set using Documentum Administrator

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.
3. Select **View > Properties**.
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 17-7: Document Set Scheduling settings**

Field	Description
Start Date	Set the day and time to indicate when the first run should happen.
Repeat	Set the frequency of the scheduling by typing a number in the <b>Repeat</b> box and selecting the time unit.

Field	Description
<b>Processing Mode</b>	For classic categorization, select the <b>Processing Mode: Production or Test</b> . If you chose <b>Test</b> , click <b>Select Taxonomy</b> and select a taxonomy to run the test against.

7. Click **OK**.
8. Synchronize the document set to make it available to the CIS server.

### 17.4.7 Synchronizing a document set using Documentum Administrator

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 Inbox.

## 17.4.8 Submitting documents to CIS server using Documentum Administrator

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 information in the *OpenText Documentum Content Intelligence Services Administration Guide*.

## 17.4.9 Submitting one document to CIS server using Documentum Administrator

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**.

## 17.4.10 Assigning a document manually using Documentum Administrator

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.

## 17.5 Managing analysis results using Documentum Administrator

### 17.5.1 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.

## 17.5.2 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.

## 17.5.3 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 check box 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 **step 3** through **step 6** to review every document for all categories for which you are the category owner.

#### 17.5.4 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.

### 17.5.5 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.

### 17.5.6 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?** check box.  
If the check box is not selected, only assignments in the current category are cleared.
6. Click **OK**.

### 17.5.7 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**.

### 17.5.8 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 check box next to its name.
3. Select **Tools > Content Intelligence > Clear Assignments**.



# Chapter 18

## Resource management

### 18.1 Understanding Resource Management

The Resource Management node provides an interface for viewing and managing resources exposed in the 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.

### 18.2 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.

## 18.2.1 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.

**!** **Important**

- In a cloud environment, if Documentum Administrator, Messaging Service, and Accelerated Content Services are deployed inside the cluster, then use the following URL format for **JMX Service URL**:

For Messaging Service:

```
service:jmx:rmi:///jndi/rmi://<IP address of Messaging Service pod or  
Messaging Service service name>:<registry port>/dms
```

For Accelerated Content Services:

```
service:jmx:rmi:///jndi/rmi://<IP address of Documentum CM Server pod or  
Accelerated Content Services service name>:<registry port>/acs
```

- If Documentum Administrator is deployed in an on-premises environment but Messaging Service is deployed in a cloud environment, then use the following URL format for **JMX Service URL**:

```
service:jmx:rmi:///jndi/rmi://<node IP of Messaging Service  
pod>:<registry node port>/dms
```

- 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.

### 18.2.2 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. Use the URL format as described in “[Adding resource agents](#)” on page 448.
  - 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.

### 18.2.3 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.

## 18.2.4 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.

## 18.3 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.
- 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.

### 18.3.1 Managing general information for resources

The Resource Properties - Info page contains general information about the resource, such as the name, status, resource agent, domain and node, and type. You can also select an interval to check the status of resources on the resource property.

**To manage general information for resources:**

1. Navigate to the Resource Properties - Info page:
  - a. Navigate to **Administration > Resource Management > Resource Agents** to access the **Resource Agents** list page.
  - b. Select the resource agent to view.
  - c. Select **View > Resources on Agent** to access the **Resources on Agent** list page that displays the resources for the selected resource agent.



**Note:** If the MBean server named in the JMX Service URL field on the Resource Agent Properties - Info page is not available, the system displays an error message instead of the Resources on Agent list page.

- d. Highlight the resource to view.
  - e. Select **View > Properties > Info** to access the **Resource Properties - Info** page.
2. View general information about the resource:
  - a. **Name:** Name of the resource
  - b. **Status:** Status of the resource.
  - c. **Resource Agent:** Name of the resource agent.
  - d. **Domain/Node:** Name of the domain or node path.
  - e. **Type:** The resource type, such as Configuration.
  - f. **Description:** Description of the resource.
3. Enter a **Polling Interval** to check the status of resources on this resource property.

If you change the polling interval on the Resource Properties - Info page, it will override the default polling interval setting on the resource agent. Default is set at 1000 milliseconds.

4. Click **OK** to save changes and return to the Resource on Agent list page or click **Cancel** to return to the Resources on Agent list page without saving any changes.

### 18.3.2 Managing resource attributes

The Resource Properties - Attributes page displays the attributes for an MBean. If the MBean enables you to update the attributes, then the system displays an input control. The MBean resource will validate the new data values.

**To manage resource attributes:**

1. Navigate to the Resource Properties - Attributes page:
  - a. Navigate to **Administration > Resource Management > Resource Agents** to access the **Resource Agents** list page.
  - b. Select the resource agent to view.
  - c. Select **View > Resources on Agent** to access the **Resources on Agent** list page that displays the resources for the selected resource agent.
  - d. Select the resource to view.
  - e. Select **View > Properties > Attributes** to access the Resource Properties - Attributes page.
2. View or modify the MBean attributes:
  - a. **Name:** Name of the attribute.
  - b. **Description:** Description of the attribute.
  - c. **Value:** Attributes may be read-only or editable.
3. Click **Refresh** to refresh the list of attributes and their values.
4. If you changed any values, click **Save Changes** to update the resource with the new values; otherwise the changes will be lost.
5. Click **OK** to save changes and return to the Resources on Agent list page or click **Cancel** to return to the Resources on Agent list page without saving any changes.

### 18.3.3 Managing resource operations

The Resource Properties - Operations page displays the operations that can be performed. Selecting an operation displays the Start Operations dialog, which enables you to enter required data (if required) and perform the operation.

**To manage resource operations:**

1. Navigate to the Resource Properties - Operations page:
  - a. Navigate to **Administration > Resource Management > Resource Agents** to access the **Resource Agents** list page.

- b. Select the resource agent to view.
  - c. Select **View > Resources on Agent** to access the **Resources on Agent** list page that displays the resources for the selected resource agent.
  - d. Select the resource that you want to view.
  - e. Select **View > Properties > Operations** to access the **Resource Properties - Operations** page.
2. Click a link in the **Name** column to access the **Start Operation** page.
  3. On the Start Operation page, enter parameters (if required) and click **Start Operation**.
  4. Click **Close** on the Start Operation page to return to the Resource Properties - Operations page.
  5. Click **OK** or **Cancel** to return to the Resources on Agent list page.

### 18.3.3.1 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 18-1: Start Operation page properties**

Field	Description
<b>Operation</b>	Name of the operation
<b>Description</b>	Description of the operation.
<b>Resource</b>	Name of the resource.
<b>Agent</b>	Name of the resource agent.
<b>Domain</b>	Domain for the resource agent.
<b>Parameters</b>	The system will display input control fields if parameters are defined for the operation.
<b>Start Operation</b>	Click to invoke the operation. The dialog box remains open until you click <b>Close</b> .
<b>Status</b>	After the operation runs, displays that the operation completed or displays an error message, if one is provided.
<b>Return Value</b>	Displays the return value of the operation, if it has one.
<b>Close</b>	Close the dialog and return to the Resource Properties - Operations page.

### 18.3.4 Viewing resource notifications

The Resource Properties - Notifications page displays the resource notifications you subscribe. These notifications are sent only while you are viewing the resource properties.

#### To view resource notifications:

1. Navigate to the Resource Properties - Notifications page:
  - a. Navigate to **Administration > Resource Management > Resource Agents** to access the **Resource Agents** list page.
  - b. Select the resource agent to view.
  - c. Select **View > Resources on Agent** to access the **Resources on Agent** list page that displays the resources for the selected resource agent.
  - d. Select the resource to view.
  - e. Select **View > Properties > Notifications** to access the **Resource Properties - Notifications** page.

The notifications shown on the Resource Properties - Notifications page occurred since you viewed the properties for this resource. Click the **Log** tab for events that occurred prior to this session.

2. Click **Refresh** to refresh the list with notifications that occurred while viewing the resource.
3. Click an item in the **Message** column to view the **Notification** page, which provides additional information about the notification for the resource.
4. Select **Subscribe** to listen for and display notifications from the resource.
5. Click **OK** or **Cancel** to return to the Resources on Agent list page.

#### 18.3.4.1 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 18-2: Fields on the Notification page**

Field	Description
<b>Message</b>	Notification message.
<b>Occurred</b>	Time notification occurred.
<b>Resource</b>	Name of the resource.
<b>Agent</b>	Name of the resource agent.
<b>Domain</b>	Domain for the resource agent.

Field	Description
<b>Close</b>	Close the dialog and return to the Resource Properties - Notifications page.

### 18.3.5 Viewing resource logs

The Resource Properties - Log page displays log file information for the resource if it is supported by the MBean resource.

**To view resource logs:**

1. Navigate to the Resource Properties - Log page:
  - a. Navigate to **Administration > Resource Management > Resource Agents** to access the **Resource Agents** list page.
  - b. Select the resource agent to view.
  - c. Select **View > Resources on Agent** to access the **Resources on Agent** list page that displays the resources for the selected resource agent.
  - d. Select the resource to view.
  - e. Select **View > Properties > Log File** to access the **Resource Properties - Log** page.

The system displays the log file name and size that the server returned.

2. Click **Download** to download the log file.

This opens a standard browser Download dialog with the log file as the download target.

3. Select a **Log Level**.

If a list of levels is published by the resource, the system displays the list of published severity levels, ranked by severity level. If no severity levels are published by the resource, the system displays all.

4. In the **View Logged Events** section, select what and how you want to view the logged events:
  - a. Select a **Severity** type to view.
  - b. Select to view the **First** or **Last** logged events and then select the number of lines to display, or select **All** to display all logged events.
5. Click **Go** to fetch the logged events from the log file using the selected criteria.
6. Click **OK** or **Cancel** to return to the Resources on Agent list page.

### 18.3.6 Monitoring resources

The <MBean name> Monitor page displays information for resource types that have been configured for the server monitor interface. The monitor interface is available only for these MBean types:

- AcsServerMonitorMBean
- AcsServerConfigMBean
- JmxUserManagementMBean
- IndexAgent

#### To monitor resources:

1. Access the <MBean name> Monitor page.
  - a. Navigate to **Administration > Resource Management > Resource Agents** to access the **Resource Agents** list page.
  - b. Select a resource agent and then select **View > Resources on Agent** to access the **Resources on Agent** list page.
  - c. Select a resource and then select **View > Monitor** to access the <MBean name> **Monitor** page.



**Note:** The Monitor menu option is available only for specific MBean types that have been configured for the server monitor interface.

2. Click **Refresh** to refresh all attributes, including writeable ones.

3. View the attributes in the **Properties** section.

You can modify the contents in the Properties section if the attributes are writeable. Click **Save Changes** to update the attributes on the MBean. After saving the changes, the system displays a message in the Notifications section if the MBean has the notifications implemented.

4. Click an operation button.

The **Start Operations** page appears where you can enter date (if required) and perform the operation.

5. View the information in the **Notifications** section.

6. View the information in the **View Logged Events** sections.

This section displays the logged events if the MBean implements these methods.

7. Click **Close** to exit and return to the Resource Agents list page.

### 18.3.6.1 Manual configuration steps for monitoring resources

This section details the manual configuration steps for monitoring resources.

#### To manually configure:

- The following changes are required in \app\webcomponent\config\admin\resourcemanagement\resources\mbeanresourceslist\_component.xml.

Add the JMXBeans to the <mbeantypes> node list.

```
<mbeantypes>
<!--name denotes the exact name of MBean-->
    <mbeantype name=IndexAgent>
        <!--onclickcomponent specifies the component to be invoked-->
            <onclickcomponent>mbeanresourcemonitordialogcontainer</onclickcomponent>
        </mbeantype>
    </mbeantypes>
```

- The following changes are required in \app\webcomponent\config\admin\resourcemanagement\resources\mbeanresourcemonitor\_component.xml.

Add the JMXBeans to the <mbeantypes> node list.

```
<mbeantypes>
<!--name denotes the exact name of the MBean-->
    <mbeantype name=IndexAgent>
<!--attributes are the list of the attributes that need
to be exposed in the monitor user interface-->
    <attributes>
        <attribute>Status</attribute>
        <attribute>Mode</attribute>
        <attribute>...</attribute>
    </attributes>
<!--operations are the list of the operations that need to be exposed
in the monitor user interface. launchcomponent=true will launch the
operations user interface in a new window. Also if the operation
requires user input, then the user interface automatically opens in a
new window-->
    <operations>
        <operation launchcomponent='false'>Start</operation>
        <operation launchcomponent='true'>downloadLogFile</operation>
        <operation launchcomponent='true'>...</operation>
    </operations>
<!--notifications are the list of notifications, ideally the
empty list will capture all notifications.-->
    <notifications>
        </notification></notification>
    </notifications>
<!--refreshinterval denotes the interval in miliseconds for the
monitor user interface to be refreshed. Ideal value should be 10sec.-->
    <refreshinterval>10000</refreshinterval>
</mbeantype>
</mbeantypes>
```



# Chapter 19

## Administrator access

### 19.1 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 OpenText Documentum CM 6 and later repositories.

Administrator access set definitions reside in the global registry. The access sets do not conflict with Documentum CM 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 who 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.

### 19.1.1 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.
2. Navigate to **Administration > Administrator Access**.  
The **Administrator Access Sets** list page appears.
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 [“Administrator access set properties” on page 460](#).
5. Click **OK** to save your changes.

**Table 19-1: Administrator access set properties**

Field	Description
<b>Name</b>	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.
<b>Description</b>	Description of the administrator access set.

Field	Description
<b>Nodes</b>	<p>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:</p> <ul style="list-style-type: none"> <li>• Basic Configuration</li> <li>• LDAP Server Configuration</li> <li>• Java Method Servers</li> <li>• User Management</li> <li>• Audit Management</li> <li>• Jobs and Methods</li> <li>• Content Objects</li> <li>• Storage Management</li> <li>• Content Delivery</li> <li>• Index Management</li> <li>• Content Intelligence</li> <li>• Content Transformation Services</li> <li>• Resource Management</li> </ul> <p> <b>Note:</b> 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 "<a href="#">Missing Content Intelligence node</a>" on page 412.</p>

Field	Description
<b>Assigned Role</b>	<p>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.</p> <p>To select or modify a role, click <b>Select</b> 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.</p> <p>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, that particular administrator access set or role combination cannot apply in that repository.</p> <p>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.</p>

### 19.1.2 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.



**Note:** The **Delete** option is disabled in a non-global repository.

#### 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.



# Chapter 20

## Client rights management

### 20.1 Client rights domains and privileged clients

A client rights domain contains the Documentum CM 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 Foundation Java API information.

Privileged DFC is the term used to refer to Foundation Java API 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.

### 20.2 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.

## 20.2.1 Creating a client rights domain

Creating a clients right 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.
2. Select **File > New > Client Rights Domain**.  
The New Client Rights Domain page displays.
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.

## 20.2.2 Enabling or disabling a client rights domain

Any modifications to a client rights domain require superuser privileges.

### To enable or disable 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 **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.

### 20.2.3 Deleting a client rights domain

Deleting a clients 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.

### 20.2.4 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.
3. Select **File > Add Member Repository**.  
The Properties page displays
4. Enter the information for the member repository as described in “[Member repository properties](#)” on page 467.
5. Click **OK** to save your changes.

**Table 20-1: Member repository properties**

Field	Description
<b>Member Repository Name</b>	The name of the repository. The repository cannot be the governing repository (global registry).

Field	Description
<b>Login Name</b>	The login name of the repository user. The user must have system administrator privileges and be a member of the dm_sysadmin group.
<b>Password</b>	The password of the repository user.
<b>User Login Domain</b>	The name of the login domain for the user. Optional property.
<b>Application Alias Name</b>	The application name for the Foundation Java API instance. Optional property.

## 20.2.5 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. Documentum CM Server does not validate the domain or the login name. The new values are saved, even if they are invalid.

4. Click **OK**.

## 20.2.6 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**.

## 20.3 Privileged clients

Privileged DFC is the term used to refer to Foundation Java API instances that are recognized by Documentum CM 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 Foundation Java API 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 Foundation Java API has an identity, with a unique identifier extracted from the PKI credentials. The first time an installed Foundation Java API is initialized, it creates its PKI credentials and publishes its identity to the global registry known to the Foundation Java API. 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 Foundation Java API 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 20-2: Privileged Clients page information**

Field	Description
<b>Client Name</b>	The name of the Foundation Java API client.
<b>Client ID</b>	A unique identifier for the Foundation Java API client.
<b>Host Name</b>	The name of the host on which the Foundation Java API client is installed.
<b>Approved</b>	Indicates if the given Foundation Java API client is approved to perform privilege escalations.
<b>Manage Clients</b>	The Manage Client button displays the Manage Client page, which lists all Foundation Java API clients that are registered in the global registry.

### 20.3.1 Adding Privileged DFC clients

The **Manage Clients** page displays the list of Foundation Java API clients created in the repository. When you select one or more Foundation Java API clients as a Privileged DFC client, a Foundation Java API 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 20-3: Manage Clients page information**

<b>Field</b>	<b>Description</b>
<b>Client Name</b>	The name of the Foundation Java API client.
<b>Client ID</b>	A unique identifier for the Foundation Java API client.
<b>Host Name</b>	The name of the host on which the Foundation Java API client is installed.
<b>Creation Date</b>	The creation date of the Foundation Java API client.

3. To search for a Foundation Java API client, enter the name, or a portion of the name of the Foundation Java API client in the search field, then click the right arrow icon.  
The system displays all registered Foundation Java API clients that match the criteria that you entered.
4. Select the registered Foundation Java API clients that you want to add as privileged clients, then click the right arrow icon.  
The selected Foundation Java API clients move to the right side.
5. Click **OK** to return to the Privileged Clients list page.

### 20.3.2 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 “[Privileged client properties](#)” on page 472.

**Table 20-4: Privileged client properties**

Field	Description
<b>Client Name</b>	The name of the Foundation Java API client.
<b>Client ID</b>	The unique identifier for the Foundation Java API client.
<b>Host Name</b>	The name of the host on which the Foundation Java API client is installed.
<b>Client Privilege</b>	Indicates whether the Foundation Java API client is approved to perform privilege escalations.
<b>Trusted Login</b>	Specifies whether the client is allowed to create sessions for users without user credentials.  Select this option to enable the client to create sessions for users without credentials.
<b>Trusted Server Privilege</b>	Specifies whether the Foundation Java API client is part of a trusted Documentum CM Server domain. If this option is enabled, the client has direct access to the repositories on the server.
<b>Is globally managed</b>	Select to propagate the privileged Foundation Java API information by domain. Optional property.
<b>Application Name</b>	The application name for the Foundation Java API instance. Optional property.

### 20.3.3 Approving or denying privileged clients

Foundation Java API 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 Foundation Java API client does not appear on the **Privileged Clients** list page, click **Manage Clients** to access the **Manage Clients** page and add the Foundation Java API client, as described in “[Adding Privileged DFC clients](#)” on page 470.

3. To approve a Privileged DFC client, select the Foundation Java API 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 Foundation Java API client and do one of the following:
  - Select **Tools > Deny Privilege**.
  - Right-click and select **Deny Privilege**.

#### 20.3.4 Deleting a Foundation Java API client and certificate

Use the instructions in this section to delete a Foundation Java API client and the certificate. You cannot delete a certificate that is also used by another Foundation Java API client.

##### To delete a Foundation Java API client and certificate:

1. Navigate to **Administration > Client Rights Management > Privileged Clients** to access the **Privileged Clients** list page.
2. Select the Foundation Java API 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 21

## Data visualization

### 21.1 Configuring reporting servers

Use the instructions in this section to configure the reporting servers.

**To configure reporting servers:**

1. Navigate to **Administration > Data Visualization > Reporting Servers**.

The **Reporting Servers** list page appears that lists all the available reporting servers along with the name, URL, and description.

You can add or modify (use the **Properties** from the shortcut menu) or delete reporting servers.



#### Notes

- The **Data Visualization** node is visible only if DA is connected to the 16.4 or later repository. If you want to have DVR functionality available on previous versions of the repositories, then you have to manually create a new object type `dm_reporting_server_config` in the repository using the following DQL:

```
CREATE TYPE "dm_reporting_server_config" ("url" string(200),  
"description" string(200)) WITH SUPERTYPE "dm_sysobject"
```

- You can add or modify or delete reporting servers only if you are connected to the global registry repository. After the reporting servers are added into the global registry repository, you can login using DA to any other repository and open the reporting server portal page to run the reports.

2. Click the reporting server name.

This connects to the iHub server and opens the main portal page of the iHub server.

You can navigate to the appropriate folder where the reports are published and view, export, schedule reports, and so on.

## 21.2 Viewing and running reports

Use the instructions in this section to view and run the reports.

### To view and run reports:

1. Navigate to **Administration > Data Visualization > Reporting Servers**.  
The **Reporting Servers** list page appears that lists all the available reporting servers along with the name, URL, and description.
2. Click the reporting server URL link.
3. Log in to the iHub server using the OpenText Documentum CM credentials.  
Ensure that the OpenText Documentum CM user is mapped with the iHub user. *OpenText Documentum Content Management - Server and Server Extensions Installation Guide (EDCSY250400-IGD)* provides the detailed instructions.
4. Navigate to the DVR folder and subfolders (if any) that contains the category of reports.
5. Click the name of the category of report. For example, `RepositoryObjectReports`.
6. Click the name of the Out-Of-The-Box (OOTB) report. For example, `LargestDocsByName`.

The report is run and displayed.



### Notes

- If the OOTB report has any parameters, the **Parameters** page appears. In the **Parameters** page, provide the details and click **Finish** to run the report.
- You can also log in to the iHub server directly using the iHub portal URL (for example, `http://<IP address of the iHub server>:8700/iportal`) in the supported browsers without Documentum Administrator. If you choose this option to log in to the iHub server, you can perform all operations other than running the DVR OOTB reports.

## 21.3 OOTB reports

### 21.3.1 Repository objects reports

Repository Objects reports display details about documents that have the maximum size. This family of reports has the following common report parameters:

- *Top <N> Records*: Displays the top <N> records fetched from the repository, where N is a whole number that specifies the number of records to be displayed.
- *Size*: It is the Fact/Measure for the Repository Objects family of reports except for the following reports which have Count as the Fact/Measure:
  - Document and Version Count by Creation Date
  - Document and Version Count by Object Type
  - Documents with Most Version Count
- *Chart*: Pie charts that display the following data:
  - Total space taken by each document type
  - Count of elements for each document type

The following table lists various OOTB reports that belong to this family of reports:

**Table 21-1: Repository objects reports**

Name of the OOTB report	Query	Query description
Largest Documents by Document Name	<pre>select object_name,        r_content_size,        a_content_type,        owner_name,        r_creation_date       from dm_document (all)      where r_content_size &gt; 0        and UPPER(object_name) like           UPPER('?%Document Name%')     ORDER BY r_content_size DESC enable (return_top {? Top N Records})</pre>	This DQL returns top 'N' largest documents with content size > 0 with the owner name, creation date, object name (specified by the object name parameter).
Largest Elements by Cabinet	<pre>select object_name,        r_content_size,        a_content_type,        r_object_type,        r_creation_date,        owner_name       from dm_sysobject (all)      where r_content_size &gt; 0        and cabinet('/?Cabinet',DESCEND) ORDER BY            r_content_size DESC</pre>	This DQL returns the top 'N' largest elements in the cabinet (specified by the cabinet parameter), or in the descendant cabinets.
Largest Documents by Folder	<pre>select object_name,        r_content_size,        a_content_type,        r_creation_date,        owner_name       from dm_document (ALL)      where r_content_size &gt; 0        and folder ('?Folder Name', DESCEND) ORDER BY            r_content_size DESC enable               (return_top {?Top N Records})</pre>	This DQL returns the top 'N' largest documents in the folder (specified by the folder parameter) or the descendant folders.

Name of the OOTB report	Query	Query description
Largest Elements by Folder	<pre>select a_content_type,r_object_type , object_name, r_content_size, owner_name, r_creation_date from dm_sysobject (ALL) where r_content_size &gt; 0 and folder ('{?Folder Name}',DESCEND) ORDER BY r_content_size DESC enable (return_top {?Top N Records})</pre>	This DQL returns the top 'N' largest elements in the folder (specified by the folder parameter) or the descendant folders.
Largest Element by Virtual Document	<pre>select r_object_id, object_name, r_content_size, a_content_type, r_object_type, r_creation_date, owner_name from dm_sysobject (all) where (r_is_virtual_doc=1 OR r_link_cnt &gt; 0) and UPPER (object_name) like UPPER ('%{?VDM}%')</pre>	This DQL returns elements with r_is_virtual_doc = 1 or r_link_cnt > 0 and object name (specified by the object name parameter).
Document and Version Count by Creation Date	<pre>select r_creation_date,count(r_version_label) as VERSION_COUNT,object_name,owner_name,r_object_type from dm_document(all) where r_creation_date &gt; DATE('? CreationDate 00:00:00','MM/ DD/YYYY hh:mm:ss') AND dm_document.i_chronicle_id=d m_document.i_chronicle_id group by object_name,r_creation_date, owner_name,r_object_type order by 1 DESC</pre>	This DQL returns documents and their version counts based on the creation date.
Document and Version Count by Object Types	<pre>select r_creation_date,count(r_version_label) as VERSION_COUNT,object_name,owner_name,r_object_type,i_contents_id from dm_document(all) where dm_document.i_chronicle_id=d m_document.i_chronicle_id AND r_object_type=? objectType[0] OR r_object_type =? objectType[1].. OR r_object_type =? objectType[n] group by object_name,r_object_type,owner_name,r_creation_date,i_contents_id order by 1 DESC</pre>	This DQL returns documents and their version counts based on the object types.

Name of the OOTB report	Query	Query description
Documents with Most Version Count	<pre>select count(r_version_label) as CNT, object_name,owner_name,r_object_type,r_creation_date from dm_document (all) where dm_document.i_chronicle_id=d m_document.i_chronicle_id group by object_name,owner_name,r_object_type,r_creation_date order by 1 DESC enable(return_top {?Top N Records})</pre>	This DQL returns documents in the order of most version counts.
Total Content Size by Cabinet	<pre>select object_name, a_content_type,r_object_type , r_content_size from dm_document (ALL) where cabinet('/{?Cabinet Name}',DESCEND) order by a_content_type</pre>	This DQL returns the content size of objects based on cabinet name (specified by the cabinet parameter)
Total Content Size by Formats	<pre>select object_name,r_content_size,a_content_type from dm_document(all) where r_content_size&gt;0 AND a_content_type in(?Formats) ORDER BY a_content_type</pre>	This DQL returns the content size of objects based on the formats.
Total Content Size by Object Types	<pre>select object_name,r_object_type,r_content_size from dm_document(all) where r_content_size&gt;0 AND r_object_type=? objectType[0] OR r_object_type =? objectType[1].. OR r_object_type =? objectType[n] ORDER BY r_object_type</pre>	This DQL returns the content size of objects based on the types.

Let us consider *Largest Document by Document Name* report as an example, in this category of reports.

This report displays the following information:

- *Top <N> largest documents having Document Name as a filter (in tabular format)*
- *Count of elements for each document type (as a pie chart): Facts/measures, for this chart, are content type and number of documents in each type.*
- *Total space taken by each document type (as a pie chart): Facts/measures, for this chart, are content type and sum of content size.*

### 21.3.2 Workflow reports

Workflow reports display details pertaining to workflows, current state of workflows, start and end dates, and details about Workflow owner. This family of reports has the following common report parameters:

- *Workflow*: It is the Dimension for the Workflow family of reports.
- *Chart*: Pie chart for displaying *Count of workflows by workflow state*.

The following table lists various OOTB reports that belong to this family of reports:

**Table 21-2: Workflow reports**

Name of the OOTB report	Query	Query description
All Outstanding Workflow Actions	<pre>select object_name, r_creation_date, r_due_date, r_performer_name,w_item.r_runtime_state from dm_workflow,dmi_workitem w_item where r_object_id=r_workflow_id and dm_workflow.r_runtime_state in(1,3) and w_item.r_runtime_state in(?WorkflowStates)</pre>	This DQL contains query for the Workflows in Dormant, Acquired, Finished, Paused, Dpaused, and Apaused states.
All Workflows in Process	<pre>select object_name,r_runtime_state, r_start_date, supervisor_name FROM dm_workflow where r_runtime_state in(0,1,3)</pre>	This DQL contains query for all Workflows in process (Dormant, Running, and Halted states).
All Workflows and their Owner	<pre>select object_name, r_creator_name, supervisor_name, r_start_date from dm_workflow</pre>	This DQL selects object, creator, supervisor, and start date from the Workflow.
Count of Workflows in process	<pre>select r_runtime_state, count(*) FROM dm_workflow where r_runtime_state in(0,1,3) GROUP BY r_runtime_state</pre>	This DQL contains query for all Workflows that are in Dormant, Active, and Halted states.
All Workflows and their well known states	<pre>select object_name, r_start_date, r_runtime_state from dm_workflow where r_runtime_state in(?WorkflowStates) GROUP BY r_runtime_state, object_name,r_start_date</pre>	This DQL contains query for Workflow such as Dormant, Active, Finished, Halted, and Failed.

Let us consider *All outstanding workflow actions* report as an example, in this category of reports.

This report displays the following information:

- *All outstanding workflow actions* having *Workflow State* as a filter (in tabular format)
- *Count of workflows by workflow state* (as a pie chart): Facts/measures, for this chart, is count of workflow states.

### 21.3.3 Retention Management reports

Retention Management reports specify details on retention policy objects.

The following table lists various OOTB reports that belong to this family of reports:

**Table 21-3: Retention Management reports**

Name of the OOTB report	Query	Query description
Qualification Manager	<pre> select a.r_object_id, a.phase_name, a.entry_date, a.event_date, a.qualification_date, s.r_version_label, s.r_is_virtual_doc, s.r_link_cnt, s.a_content_type,s.r_has_frn_assembly, s.i_is_reference, s.i_is_replica, r.object_name as policy_name, s.object_name as retained_object_name, s.r_object_type as retained_object_type, s.r_object_id as retained_object_id from dm_sysobject (all) s, dmc_rps_retainer a, dmc_rps_phase_rel b, dmc_rps_retention_strategy c, dmc_rps_retention_policy r where (any s.i_retainer_id is not null) and (a.retainer_root_id = s.r_object_id) and (a.retention_policy_id = r.r_object_id) and (a.r_policy_id = b.parent_id) and (a.retention_policy_id = b.child_id) and (a.phase_name = b.phase_name) and (not (a.event_date is nulldate and b.r_object_id in (select parent_id from dm_relation where relation_name = 'dmc_rps_phase_condition_rel_type'))) and (b.r_object_id in (select parent_id from dm_relation where relation_name = 'dmc_rps_phase_authority_rel_type' and child_id in (select r_object_id from dmc_rps_authority where is_authority_valid = TRUE))) and (a.qualification_date is nulldate) and (a.retention_policy_id = r.r_object_id) and (r.retention_strategy_id = c.r_object_id) and (not (s.r_object_type in (select r_type_name from dmi_type_info where any r_supertype = 'dm_folder') and c.is_container_aging = 0)) and (s.r_version_label != 'CURRENT') enable (ROW_BASED) </pre>	<p>This query displays a list of objects under retention, which can be manually qualified for promotion if the retention policy has been changed.</p> <p>This DQL performs the following tasks:</p> <ul style="list-style-type: none"> <li>Fetch all phases related to the current retainer's retention policy (a.retention_policy_id=b.child_id)</li> <li>Fetch the policy used to create the retention policy (a.r_policy_id=b.parent_id)</li> <li>Fetch the current phase of the retention policy (a.phase_name=b.phase_name)</li> <li>Check if the current phase has any condition. If yes, check whether the value is not null. (b.r_object_id=dm_relation.parent_id and relation_name="dmc_rps_phase_condition_rel_type") and a.event_date!= null</li> <li>Check if the current phase has valid authority (b.r_object_id = dm_relation.parent_id) and dm_relation.relation_name ="dmc_rps_phase_authority_rel_type" and child_id has an entry in dmc_rps_authority</li> <li>If the actual object type is a subtype of dm_folder, container aging (of the actual object) must be "true" (is_container_aging!=0)</li> </ul>

Name of the OOTB report	Query	Query description
		<ul style="list-style-type: none"><li>• Check if the version label of the retained object is not CURRENT (s.r_version_label != 'CURRENT')</li><li>• Enable (ROW_BASED) is a DQL hint because r_version_label is a multi-valued attribute.</li></ul>

Name of the OOTB report	Query	Query description
Promotion Manager	<pre> select     a.r_object_id,     s.r_version_label,     s.object_name,     s.r_is_virtual_doc,     s.r_link_cnt,     s.a_content_type,     s.r_object_id,     s.r_has_frzn_assembly,     s.i_is_reference,     s.i_is_replica,     a.phase_name,     a.entry_date,     a.event_date,     a.global_event_date,     a.qualification_date,     s.r_object_type,     a.retainer_root_id,     b.is_final_phase,     c.is_container_aging,     r.object_name as     policy_name from     dm_sysobject (all) s,     dmc_rps_retainer a,     dmc_rps_phase_rel b,     dmc_rps_retention_strategy     c, dmc_rps_retention_policy     r where     (any s.i_retainer_id is not     null) and     (NOT ANY     s.dmc_markup_coordinator.markup_retainer_id IN (select     r_object_id from     dmc_rps_markup_retainer     where is_freeze=TRUE)) and     (NOT ANY     s.dmc_folder_markup_coordinator.markup_retainer_id IN     (select r_object_id from     dmc_rps_markup_retainer     where is_freeze=TRUE)) and     (NOT ANY     s.dmc_lso_markup_coordinator.markup_retainer_id IN     (select r_object_id from     dmc_rps_markup_retainer     where is_freeze=TRUE)) and     (a.qualification_date is     not nulldate) and     (a.retainer_root_id =     s.r_object_id) and     (a.retention_policy_id =     r.r_object_id) and     (r.retention_strategy_id =     c.r_object_id) and     (not (s.r_object_type in     (select distinct     r_type_name from     dmi_type_info where any     r_supertype = 'dm_folder')     and c.is_container_aging =     0)) and     (a.r_policy_id =     b.parent_id) and     (a.retention_policy_id =     </pre>	<p>This query displays the list of objects under retention, which can be promoted from one phase to the next or can be disqualified after it has been qualified for promotion.</p> <p>This DQL performs the following tasks:</p> <ul style="list-style-type: none"> <li>Check if the object contains at least one retainer (any s.i_retainer_id is not null)</li> <li>Fetch the actual object of each retainer object (a.retainer_root_id = s.r_object_id)</li> <li>Check if the retainer is qualified for the next phase (a.qualification_date is not nulldate)</li> <li>Fetch the current retainer object's retention policy (a.retention_policy_id = r.r_object_id )</li> <li>Fetch the valid strategy ID given in the current retention policy (r.retention_strategy_id=c.r_object_id)</li> <li>Check if the actual object type is a subtype of dm_folder. If yes, container aging (of the object) must be "true". (not(s.r_object_type in (select r_type_name from dmi_type_info where any r_supertype = 'dm_folder') and c.is_container_aging=0))</li> <li>Fetch all phases of the current retention policy (a.r_policy_id=b.parent_id)</li> <li>Fetch the current phase of the retainer</li> </ul>

Name of the OOTB report	Query	Query description
	<pre> b.child_id) and (a.phase_name = b.phase_name) and (b.is_final_phase = 0) and (s.r_version_label != 'CURRENT') union select a.r_object_id, s.r_version_label, s.object_name, s.r_is_virtual_doc, s.r_link_cnt, s.a_content_type, s.r_assembled_from_id, s.r_has_frzn_assembly, s.i_is_reference, s.i_is_replica, a.phase_name, a.entry_date, a.event_date, global_event_date, a.qualification_date, s.r_object_type, a.retainer_root_id, b.is_final_phase, c.is_container_aging, r.object_name as policy_name from dm_sysobject (all) s, dmc_rps_retainer a, dmc_rps_phase_rel b, dmc_rps_retention_strategy c, dmc_rps_retention_policy r where (any s.i_retainer_id is not null) and (a.qualification_date is nulldate) and (a.global_event_date is not nulldate) and (a.retainer_root_id = s.r_object_id) and (a.retention_policy_id = r.r_object_id) and (r.retention_strategy_id = c.r_object_id) and (not (s.r_object_type in (select distinct r_type_name from dmi_type_info where any r_supertype = 'dm_folder') and c.is_container_aging = 0)) and (a.r_policy_id = b.parent_id) and (a.retention_policy_id = b.child_id) and (a.phase_name = b.phase_name) and (b.is_final_phase = 0) and (s.r_version_label != 'CURRENT') and (( r.r_object_id in ( select parent_id from dm_relation where </pre>	<p>(a.phase_name=b.phase_name)</p> <ul style="list-style-type: none"> <li>Check if the current phase is not the final phase</li> </ul> <p>(b.is_final_phase = 0)</p> <ul style="list-style-type: none"> <li>Check if the version label of the retained object is not CURRENT.</li> </ul> <p>(s.r_version_label != 'CURRENT')</p> <ul style="list-style-type: none"> <li>Enable (ROW_BASED) is a DQL hint because r_version_label is a multi-valued attribute.</li> </ul> <p><b>UNION</b></p> <ul style="list-style-type: none"> <li>Check if the object contains at least one retainer object</li> </ul> <p>(any s.i_retainer_id is not null)</p> <ul style="list-style-type: none"> <li>Check if the retainer is qualified for the next phase</li> </ul> <p>(a.qualification_date is not nulldate)</p> <ul style="list-style-type: none"> <li>Check if the retainer has any global event date mentioned</li> </ul> <p>(a.global_event_date is not nulldate)</p> <ul style="list-style-type: none"> <li>Fetch the actual object of each retainer object</li> </ul> <p>(a.retainer_root_id = s.r_object_id)</p> <ul style="list-style-type: none"> <li>Fetch the retention policy of the current retainer object</li> </ul> <p>(a.retention_policy_id = r.r_object_id)</p> <ul style="list-style-type: none"> <li>Fetch the strategy ID (if valid) given in the current retention policy</li> </ul> <p>(r.retention_strategy_id=c.r_object_id)</p> <ul style="list-style-type: none"> <li>Check if the actual object type is a subtype of dm_folder. If yes,</li> </ul>

Name of the OOTB report	Query	Query description
	<pre> relation_name = 'dmc_rps_ret_policy_authority_rel' and child_id in ( select r_object_id from dmc_rps_authority where is_authority_valid = TRUE ))) enable (ROW_BASED) </pre>	<p>container aging (of the object) must be “true”.</p> <p>(not(s.r_object_type in (select r_type_name from dmi_type_info where any r_supertype='dm_folder') and c.is_container_aging=0))</p> <ul style="list-style-type: none"> <li>Fetch all phases of the current retention policy</li> </ul> <p>(a.r_policy_id=b.parent_id)</p> <ul style="list-style-type: none"> <li>Fetch the current phase of the retainer object</li> </ul> <p>(a.phase_name=b.phase_name)</p> <p>(a.phase_name=b.phase_name)</p> <ul style="list-style-type: none"> <li>Check if the current phase is not the final phase</li> </ul> <p>(b.is_final_phase = 0)</p> <ul style="list-style-type: none"> <li>Check if the current phase of the retainer has valid authority</li> </ul> <p>(b.r_object_id = dm_relation.parent_id) and</p> <p>dm_relation.relation_name</p> <p>=”dmc_rps_phase_authority_rel_type” and child_id has an entry in dmc_rps_authority.</p> <p>((r.r_object_id in (select parent_id from dm_relation where relation_name = 'dmc_rps_ret_policy_authority_rel' and child_id in (select r_object_id from dmc_rps_authority where is_authority_valid = TRUE))))</p> <ul style="list-style-type: none"> <li>Check if the version label of the retained object is not CURRENT.</li> </ul> <p>(s.r_version_label != 'CURRENT')</p> <ul style="list-style-type: none"> <li>Enable (ROW_BASED) is a DQL hint because r_version_label is a multi-valued attribute.</li> </ul>

Name of the OOTB report	Query	Query description
Disposition Manager	<pre> select a.r_object_id, a.retainer_root_id, d.r_object_type, d.object_name, d.r_object_id as object_id, c.object_name as policy_name, a.qualification_date, c.disposition_strategy_id, b.object_name as disposition_strategy, a.disposition_status, a.disposition_export_location, a.is_promote_global as global_promotion, d.a_content_type, d.r_link_cnt, d.r_is_virtual_doc, d.r_has_frzn_assembly, d.i_is_replica, d.i_is_reference, d.r_lock_owner, a.approval_required, a.approval_status, dmc_prm_physical_proxy.export_state, dmc_prm_physical_proxy.destruction_state from dm_sysobject (ALL) d, dmc_rps_retainer a, dmc_rps_retention_policy c, dmc_rps_disp_strategy b where d.r_lock_owner is nullstring and a.r_object_id in (select i_retainer_id from dm_sysobject where r_object_id=a.retainer_root_id) and a.disposition_status in (0,2,-1,1) and a.qualification_date is not nulldate and (true=(select is_final_phase from dmc_rps_phase_rel where a.current_phase_id=r_object_id)) and (0&lt;(select count(au.r_object_id) from dmc_rps_authority au where au.is_authority_valid=true and au.r_object_id in (select child_id from dm_relation where relation_name = 'dmc_rps_phase_authority_rel_type' and parent_id = a.current_phase_id))) and c.disposition_strategy_id=b.r_object_id and a.retention_policy_id=c.r_object_id and a.retainer_root_id = d.r_object_id and a.retainer_root_id in (select r_object_id from dm_sysobject (ALL) where NOT ANY i_retainer_id IN (select r_object_id from dm_sysobject (ALL) where i_retainer_id=d.r_object_id)) </pre>	<p>This query displays a list of objects that are in the final phase of their lifecycle. These objects can be permanently disposed or their content and metadata can be transferred, based on the disposition strategy specified.</p> <p>This DQL performs the following tasks:</p> <ul style="list-style-type: none"> <li>Check if the object is not locked (d.r_lock_owner is nullstring)</li> <li>Get the retainer ID of those objects who retain a sysobject. a.r_object_id in (select i_retainer_id from dm_sysobject where r_object_id=a.retainer_root_id)</li> <li>Check if the disposition_status is not completed (open, pending, incomplete) (a.disposition_status in (0,2,1))</li> <li>Check if the retainer has a qualification date (a.qualification_date is not nulldate)</li> <li>Check if the retainer object is in the final phase (true=(select is_final_phase from dmc_rps_phase_rel where a.current_phase_id=r_object_id))</li> <li>Check if the retainer object has at least one valid authority (0&lt;(select count(au.r_object_id) from dmc_rps_authority au where au.is_authority_valid=true (au.r_object_id in (select child_id from dm_relation where relation_name = 'dmc_rps_phase_authority_rel_type' and parent_id = a.current_phase_id)))) and c.disposition_strategy_id=b.r_object_id and a.retention_policy_id=c.r_object_id and a.retainer_root_id = d.r_object_id and a.retainer_root_id in (select r_object_id from dm_sysobject (ALL) where NOT ANY i_retainer_id IN (select r_object_id from dm_sysobject (ALL) where i_retainer_id=d.r_object_id))</li> </ul>

Name of the OOTB report	Query	Query description
	<pre>dmc_rps_markup_retainer where is_permanent=TRUE or is_hold=TRUE))</pre>	<ul style="list-style-type: none"> <li>• Check if the disposition strategy ID of the current retainer's retention policy is valid</li> </ul> <pre>(c.disposition_strategy_id=b.r_object_id)</pre> <ul style="list-style-type: none"> <li>• Fetch the retention policy ID of the current retainer object</li> </ul> <pre>(a.retention_policy_id = c.r_object_id)</pre> <ul style="list-style-type: none"> <li>• Fetch the actual object of the current retainer object</li> </ul> <pre>(a.retainer_root_id = d.r_object_id)</pre> <ul style="list-style-type: none"> <li>• Check if the actual object is applied with hold, freeze, or permanent markup.</li> </ul> <pre>a.retainer_root_id in (select r_object_id from dm_sysobject (ALL) where NOT ANY i_retainer_id IN (select r_object_id from dmc_rps_markup_retainer where is_permanent=TRUE or is_hold=TRUE))</pre>
Barcode Manager	<pre>select dmc_prm_physical_proxy.physical_barcode, 'NONE' as availability, 'NONE' as dest_state, 'NONE' as exp_state, dmc_prm_chargeoutable.is_available, dmc_prm_physical_proxy.destruction_state, dmc_prm_physical_proxy.export_state, dmc_prm_chargeoutable.recalldate, object_name, r_object_id, r_object_type from dm_sysobject where any r_aspect_name='dmc_prm_physical_proxy' and dmc_prm_physical_proxy.physical_barcode!= ''</pre>	This DQL returns the specified attribute information about all physical objects with which bar code information is associated.

Name of the OOTB report	Query	Query description
Physical Record	<pre> select r_object_id, r_object_type, object_name, r_link_ent, r_is_virtual_doc, r_assembled_from_id, r_has_frzn_assembly, i_is_replica, i_is_reference, r_version_label, a_content_type, dmc_prm_physical_proxy.export_state, 'NONE' as exp_state, dmc_prm_physical_proxy.destruction_state, dmc_prm_physical_proxy.is_lost, dmc_prm_physical_proxy.home_location_id, dmc_prm_physical_proxy.current_location_id, dmc_prm_physical_proxy.next_location_id, dmc_prm_chargeoutable.is_available, 'NONE' as availability, dmc_prm_chargeoutable.shipping_state, 'NONE' as ship_state from dm_sysobject where (any r_aspect_name = 'dmc_prm_physical_proxy') and ((dmc_prm_physical_proxy.export_state = 1) or (dmc_prm_physical_proxy.export_state = 2) or (dmc_prm_physical_proxy.destruction_state = 1) or (dmc_prm_physical_proxy.destruction_state = 2) or (dmc_prm_physical_proxy.export_state = 0 and dmc_prm_physical_proxy.destruction_state = 0) or (dmc_prm_chargeoutable.shipping_state = 0) or (dmc_prm_chargeoutable.shipping_state = 1) or (dmc_prm_chargeoutable.shipping_state = 2) or (dmc_prm_chargeoutable.shipping_state = 3)) </pre>	<p>This query displays physical objects regardless of whether the retainer object and the retention policy are associated with them, or not.</p> <p>This DQL fetches attribute information from the physical object</p> <p>(any r_aspect_name = 'dmc_prm_physical_proxy')</p> <p>that has any of the following states:</p> <ul style="list-style-type: none"> <li>Physical object's Export state is <i>pending</i> - 1</li> <li>Physical object's Export state is <i>processing</i> - 2</li> <li>Physical object's Destruction state is <i>pending</i> - 1</li> <li>Physical object's Destruction state is <i>destroyed</i> - 2</li> <li>Physical object's Export and Destruction states are in <i>initial</i> state - 0</li> <li>Charged out Physical object's Shipping status is <i>initial</i> - 0</li> <li>Charged out Physical object's shipping status is <i>marked for chargeout</i> - 1</li> <li>Charged out Physical object's shipping status is <i>waiting for pickup</i> - 2</li> <li>Charged out Physical object's shipping status is <i>Out</i> - 3</li> </ul>

Name of the OOTB report	Query	Query description
Library Request	<pre> select a.r_object_id,s.object_name, s.r_version_label, s.a_content_type,a.phase_name, a.disposition_status, a.entry_date, a.event_date, a.global_event_date, a.qualification_date, a.r_creation_date as application_date, s.r_object_id as sysobject_id, s.r_object_type, a.retainer_root_id, b.is_final_phase, c.is_container_aging, r.object_name as policy_name, r.disposition_strategy_id, d.object_name as disposition_strategy,s.r_loc k_owner,s.owner_name,s.r_con tent_size,s.a_content_type,s .r_is_virtual_doc,s.i.is_ref erence,s.i.is_replica,s.r_ha s_frn_assembly,s.a_compound _architecture,s.r_link_cnt from dmc_rps_retainer a, dm_sysobject (all) s, dmc_rps_phase_rel b, dmc_rps_retention_strategy c, dmc_rps_retention_policy r, dmc_rps_disp_strategy d where (a.retainer_root_id = s.r_object_id) and (a.retainer_root_id in (select r_object_id from dm_sysobject (all))) and (a.r_policy_id = b.parent_id) and (a.retention_policy_id = b.child_id) and (a.phase_name = b.phase_name) and (a.retention_policy_id = r.r_object_id and a.r_policy_id=r.retainer_lif ecycle_id) and (r.retention_strategy_id=c.r _object_id) and (not(s.r_object_type in (select r_type_name from dmi_type_info where any r_supertype='dm_folder') and c.is_container_aging=0)) and (r.disposition_strategy_id = d.r_object_id) and (s.r_version_label != 'CURRENT') order by 2 enable (ROW_BASED) </pre>	<p>This DQL fetches attribute information of incomplete library requests and contact details of the requestor as specified in the query. Each request can have one of the following states associated with it:</p> <ul style="list-style-type: none"> <li>Submitted: r_current_state =0</li> <li>Processing: r_current_state =1</li> <li>Completed: r_current_state =2</li> <li>Check if the version label of the retained object is not CURRENT (s.r_version_label != 'CURRENT')</li> <li>Enable (ROW_BASED) is a DQL hint because r_version_label is a multi-valued attribute.</li> </ul>

Name of the OOTB report	Query	Query description
Retention Report	<pre> select a.r_object_id,s.object_name, s.r_version_label,s.a_content_type,a.phase_name,a.disposition_status,a.entry_date, a.event_date,a.global_event_date,a.qualification_date,a.r_creation_date as application_date,s.r_object_id as sysobject_id, s.r_object_type,a.retainer_root_id,b.is_final_phase,c.is_container_agging,r.object_name as policy_name,r.disposition_strategy_id,d.object_name as disposition_strategy,s.r_lock_owner,s.owner_name,s.r_content_size,s.a_content_type,s.r_is_virtual_doc,s.i_is_reference,s.i_is_replica,s.r_has_frzn_assembly,s.a_compound_architecture,s.r_link_cnt from dmc_rps_retainer a,dm_sysobject (all) s, dmc_rps_phase_rel b, dmc_rps_retention_strategy c, dmc_rps_retention_policy r, dmc_rps_disp_strategy d where (a.retainer_root_id = s.r_object_id) and (a.retainer_root_id in (select r_object_id from dm_sysobject (all))) and (a.r_policy_id = b.parent_id) and (a.retention_policy_id = b.child_id) and (a.phase_name = b.phase_name) and (a.retention_policy_id = r.r_object_id and a.r_policy_id=r.retainer_lifecycle_id) and (r.retention_strategy_id=c.r_object_id) and (not(s.r_object_type in (select r_type_name from dmi_type_info where any r_supertype='dm_folder') and c.is_container_agging=0)) and (r.disposition_strategy_id = d.r_object_id) and(s.r_version_label !='CURRENT') order by 2 enable (ROW_BASED) </pre>	<p>This DQL displays information pertaining to the retained objects based on the following conditions:</p> <ul style="list-style-type: none"> <li>Fetch all objects having retainers (a.retainer_root_id = s.r_object_id)</li> <li>Check if the retainer is associated with an object (a.retainer_root_id in (select r_object_id from dm_sysobject (all)))</li> <li>Fetch all phases in the applied retention policy (a.r_policy_id = b.parent_id) and (a.retention_policy_id = b.child_id)</li> <li>Fetch only the current phase (a.phase_name = b.phase_name)</li> <li>Fetch the applied retention policy from the retainer object (a.retention_policy_id = r.r_object_id)</li> <li>Check if the retention policy ID of retainer and the lifecycle ID of retention policy are the same (a.r_policy_id=r.retainer_lifecycle_id)</li> <li>Check if the applied strategy ID is valid and fetch the strategy object (r.retention_strategy_id=c.r_object_id)</li> <li>Check if the object type is a not a subtype of dm_folder. If yes, it must have container aging condition as "true". (not(s.r_object_type in (select r_type_name from dmi_type_info where any r_supertype='dm_folder'))</li> </ul>

Name of the OOTB report	Query	Query description
		<pre> and c.is_container_aging=0)) • Check if the specified disposition strategy ID is valid  (r.disposition_strategy_i d = d.r_object_id) • Check if there is a library request for this object.  a.r_policy_id = p.r_object_id • Check if there are any objects in submitted state.  (any (p.state_type='dmc_prm_su bmitted' and p.i_state_no=(select r_current_state from dmc_prm_library_request where r_object_id=a.r_object_id ))) • Check if there are any objects in pending state.  any (p.state_type='dmc_prm_pe nding' and p.i_state_no=(select r_current_state from dmc_prm_library_request where r_object_id=a.r_object_id ))) • Check if there are any objects in Processed state.  any (p.state_type='dmc_prm_pr ocessed' and p.i_state_no=(select r_current_state from dmc_prm_library_request where r_object_id=a.r_object_id ))) </pre>

Name of the OOTB report	Query	Query description
Notification Report	<pre> select n.target_object_id, s.r_object_type as target_object_type,n.object_ name,s.r_version_label,s.a_c ontent_type, r.object_name as policy_name,ph.phase_name,ac .object_name as action_name,n.a_last_review_ date as sent_date, n.number_sent, n.r_object_id as r_object_id ,true as action_image_enabled from dmc_rps_phase_rel ph, dmc_rps_retention_policy r, dmc_rps_action ac,dmc_rps_notification n, dmc_rps_action_rel ar, dm_sysobject (all) s where ( n.target_object_id=s.r_obj ect_id ) and (ph.child_id= r.r_object_id) and (ar.r_object_id = n.action_rel_id and ph.r_object_id = ar.parent_id) and (ac.r_object_id = ar.child_id) and (s.r_version_label !='CURRENT') order by 3 enable (ROW_BASED) </pre>	<p>This query displays a list of notifications sent to contacts for objects retained based on retention policies for which an action is specified.</p> <p>This DQL specifies the following actions:</p> <ul style="list-style-type: none"> <li>Fetch all objects which must be notified (n.target_object_id=s.r_object_id )</li> <li>Fetch all (notification) action objects, which are applied on the retention policy phases (ar.r_object_id = n.action_rel_id and ph.r_object_id = ar.parent_id)</li> <li>Check if actions are present in the list of actions (ac.r_object_id = ar.child_id)</li> <li>Check if the version label of the retained object is not CURRENT (s.r_version_label != 'CURRENT')</li> <li>Enable (ROW_BASED) is a DQL hint because r_version_label is a multi-valued attribute.</li> </ul>

Name of the OOTB report	Query	Query description
Retention Markup Review	<pre> select n.target_object_id, s.r_object_type as target_object_type, n.object_name,s.a_content_ty pe, ar.trigger_reason as review_reason, rm.object_name as markup_name, ac.object_name as action_name,ar.trigger_perio d as review_period, 'NONE' as rev_period, ar.trigger_month as review_month, ar.trigger_day as review_day, n.number_sent, rm.r_object_id as rm_object_id, n.r_object_id as r_object_id from dmc_rps_notification n, dmc_rps_action_rel ar, dmc_rps_action ac, dmc_rps_retention_markup rm, dm_sysobject (all) s where (n.target_object_id=s.r_obje ct_id) and (ar.r_object_id = n.action_rel_id) and (ac.r_object_id = ar.child_id) and (rm.r_object_id = ar.parent_id) order by 3 </pre>	<p>This query displays the list of objects retained by retention policies, which have <i>Review</i> selected as a Disposition Strategy.</p> <p>This DQL specifies the following actions:</p> <ul style="list-style-type: none"> <li>Fetch all the objects which must be notified (n.target_object_id=s.r_object_id)</li> <li>Fetch all phases which must be notified (ar.r_object_id = n.action_rel_id)</li> <li>Check if the actions that are present in the notification list are also specified in the list of actions (ac.r_object_id = ar.child_id)</li> <li>Check if Review is specified in the notification list of an object (rm.r_object_id = ar.parent_id)</li> </ul>

### 21.3.4 Administrative reports

Administration reports specify details to administration. This family of reports has the following common report parameter:

- *Chart*: Pie chart for displaying *Count of Users by privileges*.

The following table lists various OOTB reports that belong to this family of reports:

**Table 21-4: Administrative reports**

Name of the OOTB report	Query	Query description
Registered User	<pre>select user_name,user_state,user_lo gin_name,user_privileges from dm_user where user_state=0 and user_privileges in(0,1,2,4,8,16,3,7, 17,6,10,18,12,20,24, 9,19,15,23,31)</pre>	<p>This DQL contains query for user details with the following user privileges:</p> <ul style="list-style-type: none"> <li>• None</li> <li>• Create Type</li> <li>• Create Cabinet</li> <li>• Create Group</li> <li>• Sysadmin</li> <li>• Superuser</li> <li>• Create Type and Create Cabinet</li> <li>• Create Type and Create Group</li> <li>• Create Type and Sysadmin</li> <li>• Create Type and Superuser</li> <li>• Create Cabinet and Create Group</li> <li>• Create Cabinet and Sysadmin</li> <li>• Create Cabinet and Superuser</li> <li>• Create Group and Sysadmin</li> <li>• Create Group and Superuser</li> <li>• Sysadmin and Superuser</li> <li>• Create Type, Create Cabinet and Sysadmin</li> <li>• Create Type, Create Cabinet and Superuser</li> <li>• Create Type, Create Cabinet, Create Group and Sysadmin</li> <li>• Create Type, Create Cabinet, Create Group and Superuser</li> <li>• Create Type, Create Cabinet, Create Group, Sysadmin and Superuser</li> </ul>

Name of the OOTB report	Query	Query description
Audit Trail	<pre>select r_object_id, event_name, user_name, object_name, object_type, version_label, time_stamp, string_1, string_2, attribute_list from dm_audittrail</pre>	This DQL returns records from the Audit Trail table.

The *Registered Users* report displays the following information:

- *All Registered Users having User Privileges* as a filter (in tabular format)
- *Count of Users by privileges* (as a pie chart): *User* is the dimension, for this chart.

## Chapter 22

# 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.

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.



**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.

## 22.1 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.

## 22.2 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.

## 22.3 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 23

# 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.

## 23.1 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**.



### Notes

- 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:

```
<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>
```

## 23.2 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.

## 23.2.1 Viewing process template properties search results

The following table describes columns of returned information about the properties of the process templates:

**Table 23-1: Process template properties fields**

Field	Description
<b>Name</b>	The name of the process as described while creating the process template.
<b>Version</b>	The version of the template.
<b>Modified</b>	Date that the template was last modified.
<b>Instances</b>	Number of workflows currently running and using this process template.
<b>Longest Duration</b>	The elapsed time of the longest running instance of this process.
<b>Audited</b>	Indicates if auditing is turned on for the process.
<b>Paused Tasks</b>	Number of tasks that have been paused.
<b>State</b>	Indicates if the template is a draft or has been validated or installed.
<b>Overdue Tasks</b>	Number of tasks that are overdue.

## 23.2.2 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.

### 23.2.2.1 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.

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.

**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 Documentum Administrator. Any changes you make to the process parameter default values in Forms Builder are ignored.

### 23.2.2.2 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 is support for Business Objects (BO) which can be added as attachments or packages. In the package selector, all the attributes of the BO will be visible making it easier for you to make a selection.

### 23.2.2.3 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](#)” on page 505 provides details on the functions available for administering process instances.

## 23.3 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.

### 23.3.1 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 23-2: Process Instance search fields**

Field	Description
<b>Workflow name</b>	The name of the process instance.
<b>Supervisor name</b>	A user with the role of supervisor for that particular instance.
<b>Process name</b>	The name of the process template.

Field	Description
<b>Runtime State</b>	<p>Select one of the following workflow states:</p> <ul style="list-style-type: none"> <li>• All</li> <li>• Running</li> <li>• Dormant</li> <li>• Halted</li> </ul> <p> <b>Note:</b> In the custom search page, the value for <b>Runtime State</b> 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</p>
<b>Version Label</b>	The version of the process template.
<b>Containing Tasks with Status</b>	<p>Select a value for the type of instances you want to appear in the search results.</p> <ul style="list-style-type: none"> <li>• All</li> <li>• Failed</li> <li>• Overdue</li> <li>• Overdue and Failed</li> <li>• Overdue or Failed</li> </ul> <p> <b>Note:</b> In the custom search page, the value for <b>View Filter</b> 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.</p>

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.

### 23.3.2 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 23-3: Buttons on Process Instances page**

Button	Description
<b>Instance View</b>	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. <a href="#">“Administering tasks” on page 507</a> provides more information on the process instance view.
<b>Change Supervisor</b>	Enables the administrator to select another supervisor from a list.
<b>Resume Workflow</b>	Starts this workflow and all its current tasks.
<b>Halt Workflow</b>	Pauses the workflow and pauses all of its current tasks.
<b>Terminate Workflow</b>	Stops the workflow without the option of restarting it.

## 23.4 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**.

**Table 23-4: Task properties**

Field	Description
<b>Task Name</b>	The name of the activity or the name of the sub-process associated with the instance.

Field	Description
<b>Status</b>	Displays the current status of the task.
<b>Action</b>	The type of action that was performed on the task. For example, if the workitem was forwarded to another user, the action is <i>Forward</i> .
<b>Performer(s)</b>	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\$.
<b>Comment(s)</b>	Any comment or notations associated with the task.
<b>Receive Date</b>	The date the task was received by the task processor.
<b>Complete Date</b>	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 23-5: Administrative actions**

Field	Description
<b>Previous</b>	Displays the previous tab of the Task Info page.
<b>Next</b>	Displays the next tab of the Task Info page.
<b>Get Task</b>	Assigns the task to you and refreshes the page, enabling you to work on the task immediately.
<b>Assign</b>	Assigns the task to another user to complete.
<b>Finish</b>	Completes the task and sends it to the next step of the activity.
<b>Delegate</b>	Assigns another user the responsibility of performing a task that originally had been assigned to you.

Field	Description
<b>Repeat</b>	Sends the task to another user or group to repeat a task that you have just completed.
<b>Perform</b>	Executes the task.
<b>Close</b>	Closes the task.
<b>Complete</b>	Finishes the task and sends it to the next user or activity in the workflow.
<b>Rerun</b>	Runs automatic activities that have failed.
<b>Reject</b>	Sends the task to another step as defined in the template.
<b>Suspend</b>	Pauses the task in order to wait for some other supporting document or task to take place.
<b>Unsuspend</b>	Removes the task from the suspended state and enables the performer to acquire the task.
<b>Unassign</b>	Returns the task to the work queue and the status of the task appears as dormant until reassigned to another user.
<b>Assign</b>	Enables you to select the next performers for the task.
<b>Reassign</b>	Enables you to assign the task to a performer again.

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 23-6: Task properties**

Field	Description
<b>Task Name</b>	The name of the activity or the name of the sub-process associated with the instance.
<b>Status</b>	Displays the current status of the task.
<b>Action</b>	The type of action that was performed on the task. For example, if the workitem was forwarded to another user, the action is <i>Forward</i> .
<b>Performer(s)</b>	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\$.
<b>Comment(s)</b>	Any comment or notations associated with the task.

Field	Description
<b>Receive Date</b>	The date the task was received by the task processor.
<b>Complete Date</b>	The date the task was completed by the processor.

The **Process Variables** tab enables Administrator to provide values to the process variables added to a process in xCP designer.

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
```

## 23.5 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.

#### 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** check box.
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.



## Chapter 24

# Cabinets, files, and virtual documents

## 24.1 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**.
3. 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 “[Permissions tab for cabinets, folders, and files](#)” on page 513.
7. Click **Finish**.

**Table 24-1: Permissions tab for cabinets, folders, and files**

Field	Description
<b>Your Permissions</b>	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.
<b>Permission Set Name</b>	The name of the default permission set that is assigned to this cabinet, folder, or file.  To change the permission set, click <b>Select</b> and select a different permission set from the permission set list.
<b>Permissions Set Owner</b>	The name of user that owns the permission set that is assigned to the cabinet, folder, or file.

Field	Description
<b>Description</b>	A description of the permission set. The default description is the object ID of the permission set.
<b>Additional Permissions</b>	<p>Specifies other users and groups that have permissions for this cabinet, folder, or file.</p> <p>By default, all users (dm_world) have a Read permission and only the cabinet, folder, or file owner (dm_owner) has a Delete permission.</p> <p>To add or change permissions:</p> <ul style="list-style-type: none"> <li>• To add users or groups, click <b>Add</b> and assign the desired permissions.</li> <li>• To change the permissions for a user or group, select the user or group and click <b>Edit</b>.</li> <li>• To remove a user or group, select the user or group and click <b>Remove</b>.</li> </ul>
<b>Restrictions</b>	<p>Specifies the access restrictions for specific users and groups. Click <b>Restriction</b> to expand and view the restricted users and groups.</p> <p>To add or change restrictions:</p> <ul style="list-style-type: none"> <li>• To add users or groups, click <b>Add</b> and assign the desired restrictions.</li> <li>• To change the restrictions for a user or group, select the user or group and click <b>Edit</b>.</li> <li>• To remove a user or group, select the user or group and click <b>Remove</b>.</li> </ul>
<b>Advanced Permissions</b>	<p>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.</p> <p>Click <b>Advanced Permission</b> to expand and view the required user and group memberships. To add a required group, click <b>Add</b> and select the group and group set.</p>
<b>Search</b>	Displays permissions for users and groups. Click <b>Search</b> and select a user or group, then click <b>OK</b> . The system displays the permissions that are currently assigned to that user or group.

## 24.2 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 ["Permissions tab for cabinets, folders, and files" on page 513](#).
6. Click **Finish**.

## 24.3 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 ["Info tab for documents" on page 515](#).
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 ["Permissions tab for cabinets, folders, and files" on page 513](#).
6. Click **Finish**.

**Table 24-2: Info tab for documents**

Field	Description
Name	Specifies the name of the document.
Type	Specifies the file type. Select a file type from the drop-down list.  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.

Field	Description
<b>Format</b>	Specifies the file format. Select a format from the drop-down list.  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.
<b>Template</b>	Specifies a file template. Select a template from the drop-down list.  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.
<b>Show Options</b>	Click to expand the Options menu. Check the <b>Subscribe to this file</b> option to receive email notifications if the file is modified.

## 24.4 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.

## 24.5 Working with files

### 24.5.1 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.

### 24.5.2 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 “[Checkin information](#)” on page 518. 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 24-3: Checkin information**

Field	Description
<b>Save as</b>	Sets the version number. Selecting the same version number overwrites the original file with the updated one.
<b>Version label</b>	Lets you label the updated version.
<b>Description</b>	Lets you write an optional description of the file.
<b>Format</b>	Defines the type of file.
<b>Lifecycle ID</b>	Assigns a lifecycle to the file.
<b>Check for links to other Microsoft documents, and check in linked documents</b>	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.

Field	Description
<b>Upload options</b>	<p>Determines how quickly the new content is available to other users, and whether you can use Documentum Administrator during the checkin operation.</p> <p> <b>Note:</b> If you used drag-and-drop, you are not given this option.</p> <p>Select one of these:</p> <ul style="list-style-type: none"> <li>• <b>Send for immediate global access:</b> Updates the repository immediately for all your organization's users. While this occurs, you cannot perform other actions in Documentum Administrator.</li> <li>• <b>Send first for local access:</b> 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.</li> </ul> <p> <b>Note:</b> If checking in multiple files using the <b>Next</b> button, this option appears only for the first file. The choice you make automatically applies to all remaining files.</p>
<b>Show Options</b>	<p>Retain Lock: Saves the updated file to the repository but keeps the file checked out in your name.</p> <p>Make this the current version: Makes the updated file the current version.</p> <p>Keep a local copy after checkin: Retains a copy of the file on your local computer. But you no longer have the file checked out, and any changes you make to the local copy have no effect on the file in the repository.</p> <p>Subscribe to this file: The file is linked to your Subscriptions.</p> <p>Check in from file: Replaces the repository file with a file you choose.</p>

### 24.5.3 Viewing checkedout 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.

### 24.5.4 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**.

### 24.5.5 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.

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.

## 24.5.6 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**.

### 24.5.7 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.

### 24.5.8 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.

## 24.5.9 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 “[Properties for imported files](#)” on page 523. 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 24-4: Properties for imported files**

Field	Description
Type	<i>Do not change this property</i>
Format	<i>Do not change this property</i>
Lifecycle ID	Assigns a lifecycle to each imported item.
<b>Check for links to other Microsoft documents, and import linked documents</b>	If this field appears, check this to have Documentum Administrator scan each imported document for linked documents. If linked documents are found, they are also imported. The original document becomes a virtual document, and the linked documents become descendants.

Field	Description
<b>Upload options</b>	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: <ul style="list-style-type: none"><li>• <b>Send for immediate global access</b> Updates the repository immediately for all your organization's users. While this occurs, you cannot perform other actions in Documentum Administrator.</li><li>• <b>Send first for local access</b> 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.</li></ul>

#### 24.5.10 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**.
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 the 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.

### 24.5.11 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**.



### Notes

- 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.

#### 24.5.11.1 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**.

#### 24.5.11.2 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**.

### 24.5.11.3 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.

### 24.5.12 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**.

## 24.6 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 delete all items at once, click **Finish**.

## 24.7 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**.

## 24.8 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**.

## 24.9 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**.

## 24.10 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.

Some rendition and transformation functionality is available only on repositories that are configured with the Transformation Services products.

### 24.10.1 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.

## 24.10.2 Transforming a document to PDF or HTML format

Documentum Administrator requires the 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 indicates that the file has a pending transformation request.
- A green indicator indicates that a transformation request is currently processing.
- A red indicator indicates that a transformation request has failed.

### 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.

## 24.10.3 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:

1. Select **Tools > Preference**.
2. Navigate to the **General** tab.
3. Select the check box for **Turn Inbox Notification options on**.

## 24.11 Configuring PDF Annotation Service

If PDF Annotation Service is installed with Documentum CM 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**.

## 24.12 Virtual documents

In a 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.

## 24.12.1 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.
2. Select **Tools > Virtual Document > Convert to Virtual Document**.

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` and `IDfSysObject.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.

## 24.12.2 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.
3. Select **Tools > Virtual Document > View Virtual Document**.

## 24.12.3 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)**.

## 24.12.4 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.
2. Select **Tools > Virtual Document > Modify Version Labels**.
3. Enter a version label.
4. To apply the version label to all descendants of the virtual document, select **apply to all descendants**.
5. Click **OK**.

## 24.12.5 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.
2. Select **Tools > Virtual Document > New Snapshot**.
3. Enter information in tabs as appropriate.
4. Click **Finish**.

### 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.

## 24.12.6 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.
4. Select **Tools > Virtual Document > Convert to Simple Document**.

## 24.12.7 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 “Virtual document preferences” on page 535.

**Table 24-5: Virtual document preferences**

Field	Description
<b>Opening options</b>	Specifies how a virtual document is opened. This option does not apply if the virtual document is already opened in Virtual Document Manager (VDM): <ul style="list-style-type: none"> <li>• <b>View structure:</b> The first level of nested files appears.</li> <li>• <b>View content:</b> A read-only copy of the content appears.</li> <li>• <b>Prompt each time:</b> The user is prompted to select to display the structure or the read-only content.</li> </ul> If there is no content in a virtual document, the VDM automatically displays the virtual document structure, regardless of the preference.
<b>Bindings</b>	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.
<b>Copy</b>	Specifies how a virtual document is copied to the clipboard: <ul style="list-style-type: none"> <li>• <b>Root only:</b> Copies the content, and properties of the parent file only.</li> <li>• <b>Root and descendants:</b> Copies the parent file, and all the descendants nested in the parent file, including descendants of descendants.</li> <li>• <b>Root and link to existing descendants:</b> Copies the parent file, and references the descendants.</li> <li>• <b>Prompt me each time:</b> Prompts the user to select what to copy.</li> </ul>

Field	Description
Checkout	Specifies how a locked virtual document is checked out: <ul style="list-style-type: none"><li>• <b>Download as read-only:</b> Downloads a copy of the item as read-only.</li><li>• <b>Prompt me each time:</b> Prompts the user to select whether to download as read-only.</li></ul>

3. Click **OK** to save the preferences.

## 24.13 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. *OpenText Documentum Webtop 6.8 User Guide* contains the detailed information.

# Chapter 25

## Inbox

### 25.1 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.

### 25.2 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.

### 25.3 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.

## 25.4 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.

### 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**.

## 25.5 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.

## 25.6 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**.

## 25.7 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**.

## 25.8 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**.

## 25.9 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 check box that changes your status to unavailable.
  - To make yourself unavailable, select the check box 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.

## 25.10 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 26

## Search

### 26.1 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 Documentum CM Server host, administrators also have the option to create search templates and configure smart navigation.

*OpenText Documentum Content Management - Server and Server Extensions Installation Guide (EDCSY250400-IGD)* provides more information about installing Federated Search Services.

### 26.2 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 Documentum CM 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**.

## 26.3 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.

## 26.4 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 search box, type the words for which to search.

*“Further define search terms” on page 545* provides the detailed information to further define your search.

2. Click the search icon.

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 the stop icon.

3. “[Viewing search results](#)” on page 554 provides the detailed information.

### 26.4.1 Further define search terms

You can use the syntax in “[Further define search terms](#)” on page 545 to further define search terms within a simple search or within the **Contains** field in an advanced search.

**Table 26-1: Further define search terms**

Syntax	Description
Quotation marks around a word or phrase: “ ”	To search for an exact word or phrase, type quotation marks around the word or phrase.  For a simple search (including the Contains field in an advanced search), if you do not use quotation marks, Documentum Administrator displays files that contain both the exact words you typed as well as variations of the words, such as <i>scanning</i> for the word <i>scanner</i> .  This option is disabled when searching for more than one word or if your repository has not been indexed for variations.  Quotation marks cannot be used to match the exact case of a word.

Syntax	Description
The <b>AND</b> and <b>OR</b> operators	<p>To get results that contain two search terms, type <b>AND</b> between the terms. A term can be a word or quoted phrase.</p> <p>To get results that contain at least one term, type <b>OR</b> between the words or the quoted phrases.</p> <p>You can string together multiple terms with the <b>AND</b> and <b>OR</b> operators. The <b>AND</b> operator has precedence over the <b>OR</b> operator. For example, if you type:</p> <p><code>knowledge or management and discovery</code></p> <p>then your results must contain either knowledge or they must contain management, and discovery.</p>

Syntax	Description
The NOT operator	<p>To get results that do not contain a term, type <b>NOT</b> before this term. The term can be a word or a quoted phrase. Only the term that follows the operator is taken into account.</p> <p>The <b>NOT</b> operator can be used after the <b>AND</b> or <b>OR</b> operator, separated by a space.</p> <p>Valid syntaxes would be: <i>Documentum NOT adapter</i> or <i>Documentum AND NOT adapter</i>, both queries will return results that contain Documentum but do not contain adapter.</p> <p>If you type <i>Documentum OR NOT adapter</i>, you get results that either contain Documentum (and possibly contain adapter) or that do not contain adapter. Use this syntax cautiously. It can generate a very large number of results.</p> <p>The <b>NOT</b> operator can be used alone at the beginning of the query. For example, if you type <i>NOT adapter</i>, you get results that do not contain adapter. Use this syntax cautiously. It can generate a very large number of results.</p> <p>The <b>NOT</b> operator is not supported for queries on external sources when it is alone at the beginning of the query or if used with the <b>OR</b> operator.</p> <p>The <b>NOT</b> operator cannot be used with parentheses. This is invalid: <i>A NOT ( B OR C )</i>. However, the <b>NOT</b> operator can be used inside parentheses. This is valid: <i>( A NOT B ) OR ( A NOT C )</i>.</p> <p>ANDNOT (in one word) is not an operator, if you enter ANDNOT in a query, it will be considered as a search term.</p>

Syntax	Description
Parentheses around terms: ()	<p>To specify that certain terms must be processed together, use parentheses. When using parenthesis, you <i>must</i> type a space before, and after each parenthesis mark, as shown here: ( <i>management or discovery</i> )</p> <p>As an example, if you type <i>knowledge and management or discovery</i>, then your results will contain both knowledge, and management <i>or</i> they will contain discovery. But if you type <i>knowledge and ( management or discovery )</i>, then your results will contain knowledge, and either management <i>or</i> discovery.</p>
The multiple-character wildcard: *	<p>If the repository is indexed, you can use the multiple-character wildcard to indicate additional characters anywhere in a word. It matches zero or more characters. The multiple-character wildcard is only available or a simple search (including the <b>Contains</b> field in an advanced search).</p> <p>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 <b>Begin with</b> operator.</p> <p>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*m*ent then your results must contain: document, development, deployment, department, etc. but not documented or documentation.</p>
The single-character wildcard: ?	<p>If the repository is indexed, you can use the single-character wildcard to indicate a single, unknown character anywhere in a word.</p> <p>The single-character wildcard is only available or a simple search (including the <b>Contains</b> field in an advanced search).</p> <p>The single-character wildcard is not available for searches on non-indexed repositories, for searches of property values, or for searches of external sources.</p>



### Notes

- The operators AND, OR, and NOT are reserved words. To search a term that includes an operator, use quotation marks. For example, if you search for "hardware and software", 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.

## 26.5 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" on page 549](#) provides the detailed information.
3. Click **Search**.



**Tip:** To stop the search, in the result page, click the stop icon.

### 26.5.1 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" on page 549](#).



**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 2.b](#) and [step 2.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. The following table 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 26-2: Common properties in an advanced search**

Field	Description
Properties list	<p>Enter one or more property values to search for by doing these:</p> <ol style="list-style-type: none"> <li>1. If no fields appear, click <b>Select a property</b>.</li> <li>2. On a given line: In the first drop-down list, select a property. In the second drop-down list, select a property-to-value relationship. “<a href="#">Select a property-to-value relationship</a>” on page 553 provides the description of possible relationships. In the remaining fields, select or type values.</li> <li>If you type multiple words, they are searched for as a phrase. For example, if you type “knowledge management” then Documentum Administrator searches for values that contain the phrase “knowledge management” but not for values that contain “knowledge” and “management” separated from each other by other words such as “knowledge and process management”. If you want your results to include both terms either as a phrase or separately, you must create two subqueries, and use the AND operator.</li> <li>3. To add additional properties, click <b>Add another property</b>, and then select one of these operators: <ul style="list-style-type: none"> <li>• <b>And:</b> Selecting this means that the search results must match both the property value on this line, and the property value on the previous line.</li> <li>• <b>Or:</b> Selecting this means that the results can match either the property value on this line or the property value on the previous line. If you search external sources, do not use the <b>OR</b> operator between different types of properties. This query is valid: “<i>Author contains Lewis OR Author contains Twain</i>,” but this query is not valid: “<i>Author contains Lewis OR Name contains Knowledge management</i>.”</li> </ul> </li> </ol>

Field	Description
	<p>If you add three or more lines of properties, the order of operations follows the order of definition. Each time you add <b>And</b> or <b>Or</b>, the previous operators are grouped together. For example, if you define the query <i>"Name contains Knowledge Management AND Author contains Lewis OR Author contains Twain,"</i> then the results either must contain the documents whose name is Knowledge Management, and whose author is Lewis or they must contain all the documents whose author is Twain. To find all the documents whose name is Knowledge management, and whose author is either Lewis or Twain, you must define the following query: <i>Author contains Lewis OR Author contains Twain AND Name contains Knowledge management.</i></p> <p>4. To remove a property from the search criteria, click <b>Remove</b> for that property.</p>
<b>Date</b>	<p>Select the type of date to search for. Specify a date range, either a fixed date range using today's date or by typing the <b>From</b> and/or <b>To</b> dates. Months can be written in figures or in full. Years can be written with two or four figures.</p> <p>When specifying a date From, the date is not included in the date range. Conversely, when specifying a date To, the date is included in the date range.</p>
<b>Size</b>	Select a size range.
<b>Properties when searching for email messages</b>	<p><b>Subject:</b> Type the words for which to search.</p> <p><b>To</b></p> <p><b>From</b></p> <p><b>Sent:</b> Select the date the email message was sent.</p> <p><b>Received:</b> Select the date the email message was received.</p>
<b>Find hidden objects</b>	Choose to include hidden items in the search. The search displays only those hidden items that you have permission to view.

Field	Description
<b>Find all versions</b>	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. The following table describes the operators available in the Advanced Search page.

**Table 26-3: Select a property-to-value relationship**

Operator	Description
<i>Relational operators:</i>	
Less than <	You can use these operators with numerical values or strings.
Less than or equal to <=	
Greater than >	
Greater than or equal to >=	
Equal to =	Returns results in which the property value contains only the exact value you typed.
Not equal <>	Returns results in which the property value never matches the value you typed.
<i>Truncation operators:</i>	
Begins with	Returns results in which the property value begins with the value you typed. Same as using an ending wildcard.
Ends with	Returns results in which the property value ends with the value you typed. Same as using an starting wildcard.
Contains	Returns results in which the property value contains the value you typed anywhere within it. Same as using starting, and ending wildcards.
Does not contain	Returns results in which the property value does not contain the value you typed anywhere within it.
<i>Other operators:</i>	
In	Returns results in which the property value matches one of the values you typed. Potential values are typed as a comma-separated list.
Not in	Returns results in which the property value does not match any of the values you typed.

Operator	Description
Is null	Returns results in which the property value is not defined. If you know that a property contains no value, you can use this operator to narrow a search.
Is not null	Returns results in which the property value is defined, but with no specific value. You can use this operator to find only documents whose properties are defined. For example, if you select keywords is not null then your results must contain only documents with keywords.

## 26.6 Viewing search results

In search results, you can do these:

- Turn highlighting on or off.
- 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” on page 555](#).
- 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” on page 563](#).
- 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” on page 564](#).
- To save results from an external source into a repository, see [“Saving search results from external sources” on page 556](#).

## 26.6.1 Smart navigation

The smart navigation feature requires that Federated Search Services is installed on Documentum CM 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](#)” on page 543.

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 refresh icon. The icon appears when new results are available.

## 26.6.2 Monitoring search results in real time

Search monitoring displays the status of your search in real-time. The real-time status appears in both animated and table display. 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.

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**.

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.

### 26.6.3 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**.

## 26.7 Running an advanced search for archiving document in InfoArchive

To search for a document by one of its properties and to archive the document in InfoArchive, use advanced search. An advanced search enables you to define more precisely your query on the properties of the document that needs to be archived in InfoArchive.

**To run an advanced search for archiving document in InfoArchive:**

1. In the Documentum Administrator main page, click the arrow next to the magnifying glass icon, and then click **Advanced**.
2. Select the **Switch to Archive Objects** option.
3. Enter values for the search.
  - a. (Optional) In the **Advanced Search: Search to Archive** page, click **Clear** to clear any existing values and start with empty fields.
  - b. In the **Contains** field, type the text for which to search.  
This field is similar to the simple search.
  - c. In **Locations**, select the locations to search.

To add locations, do these:

- i. Ensure that **Current location only** is not selected, and then click **Edit**.
- ii. 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.



**Note:** The **Available Sources** list 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.
- iii. Click the arrow to add it to the **Included in Search** list.
  - iv. Repeat [step 3.c.ii](#) and [step 3.c.iii](#) for as many locations as needed.
  - v. To remove a location, select it and click the remove arrow.
  - vi. To set the locations as your default locations for every new search, select **Set as default sources**.
  - vii. Click **OK**.
  - d. In the **Object Type** list, select the type of files to search for.
4. Enter the remaining properties as appropriate. The following table describes the common properties. The properties available depend on the type of file you search for, as selected in the **Object Type** list in [step 3.d](#).

**Table 26-4: Common properties in an advanced search for archiving document in InfoArchive:**

Field	Description
<b>Properties list</b>	<p>Enter one or more property values to search for. Perform the following tasks:</p> <ol style="list-style-type: none"> <li>1. On a given line: In the first list, select a property. In the second list, select a property-to-value relationship. <a href="#">“Select a property-to-value relationship” on page 559</a> provides the description of possible relationships. In the remaining fields, select or type values. If you type multiple words, they are searched for as a phrase. For example, if you type knowledge management, then Documentum Administrator searches for values that contain the phrase knowledge management but not for values that contain knowledge and management separated from each other by other words such as knowledge and process management. If you want your results to include both terms either as a phrase or separately, you must create two subqueries, and use the AND operator.</li> <li>2. To add additional properties, click <b>Add another property</b> and select one of these operators: <ul style="list-style-type: none"> <li>• <b>and:</b> Selecting this means that the search results must match both the property value on this line and the property value on the previous line.</li> <li>• <b>or:</b> Selecting this means that the results can match either the property value on this line or the property value on the previous line. If you search external sources, do not use the <b>or</b> operator between different types of properties. This query is valid: <i>Author contains Lewis OR Author contains Twain</i>, but this query is not valid: <i>Author contains Lewis OR Name contains Knowledge management</i>.</li> </ul> </li> </ol> <p>If you add three or more lines of properties, the order of operations follows the order of definition. Each</p>

Field	Description
	<p>time you add <b>and</b> or <b>or</b>, the previous operators are grouped together. For example, if you define the query “<i>Name contains Knowledge Management AND Author contains Lewis OR Author contains Twain</i>,” then the results either must contain the documents whose name is Knowledge Management and whose author is Lewis or they must contain all the documents whose author is Twain. To find all the documents whose name is Knowledge management and whose author is either Lewis or Twain, you must define the following query: <i>Author contains Lewis OR Author contains Twain AND Name contains Knowledge management</i>.</p> <p>3. To remove a property from the search criteria, click <b>Remove</b> for that property.</p>
<b>Date</b>	<p>Select the type of date to search for. Specify a date range, either a fixed date range using today’s date or by typing the <b>From</b> and/or <b>To</b> dates. Months can be written in figures or in words. Years can be written with two or four figures.</p> <p>When specifying a date <b>From</b>, the date is not included in the date range. Conversely, when specifying a date <b>To</b>, the date is included in the date range.</p>

The relationship between a property and its corresponding value is defined by operators. The following table describes the operators available in the Advanced Search page.

**Table 26-5: Select a property-to-value relationship**

Operator	Description
<i>Relational operators:</i> Less than < Less than or equal to <= Greater than > Greater than or equal to >=	You can use these operators with numerical values or strings.
Equal to =	Returns results in which the property value contains only the exact value you typed.

Operator	Description
Not equal <>	Returns results in which the property value never matches the value you typed.
<i>Truncation operators:</i>	The truncation operators can be used in place of the multiple-character wildcard.
Begins with	Returns results in which the property value begins with the value you typed. This is similar to as using an ending wildcard.
Ends with	Returns results in which the property value ends with the value you typed. This is similar to as using an starting wildcard.
Contains	Returns results in which the property value contains the value you typed anywhere within it. This is similar to as using starting and ending wildcards.
Does not contain	Returns results in which the property value does not contain the value you typed anywhere within it.
<i>Other operators:</i>	
In	Returns results in which the property value matches one of the values you typed. Potential values are typed as a comma-separated list.
Not in	Returns results in which the property value does not match any of the values you typed.
Is null	Returns results in which the property value is not defined. If you know that a property contains no value, you can use this operator to narrow down a search.
Is not null	Returns results in which the property value is defined, but with no specific value. You can use this operator to find only documents whose properties are defined. For example, if you select keywords is not null, then your results must contain only documents with keywords.

5. Click **Search**.

 **Tip:** To stop the search, in the result page, click the stop icon.

## 26.8 Viewing search results and archiving document in InfoArchive

In search results, you can do these:

- To run the search again without revising it, click **Restart**.
- To archive the document in InfoArchive, see “[Archiving document in InfoArchive](#)” on page 561.
- To revise the search and run it again, click **Edit**, set values, and click **Search**.
- To save the search so that it can be run again to receive updated results, see “[Saving a search](#)” on page 563.
- 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](#)” on page 564.
- Turn highlighting on or off.
- 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. “[Smart navigation](#)” on page 555 provides more information.

### 26.8.1 Archiving document in InfoArchive

#### To archive document in InfoArchive:

1. Select the document from the search results.



**Note:** You can also select multiple documents.

2. To archive the document in InfoArchive, do one of the following tasks:
  - Click **Archive** next to the **Restart** option.
  - Select **File > Archive**.
  - Right-click the document and select **Archive**.
3. Click **OK**.

## 26.9 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.

## 26.10 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:

- search icon with an eye on it means this saved search is public, and accessible to any user.
- search icon with a star on it 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 search icon.

### 26.10.1 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.

## 26.10.2 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**.



**Tip:** To stop the search, in the result page, click **Stop**.

## 26.10.3 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**.

## 26.11 Creating a search template

If Federated Search Services is installed on Documentum CM 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:

- search icon with an eye on it means this search template is public, and accessible to any user.
- search icon with a star on it 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.

*OpenText Documentum Content Management - Server and Server Extensions Installation Guide (EDCSY250400-IGD)* 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**.



# Chapter 27

## Tools

### 27.1 The Tools menu

#### 27.1.1 API and DQL

DQL queries and server APIs can be run from Documentum Administrator pages that contain a Tools menu. 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.

### 27.2 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.

#### 27.2.1 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.

## 27.2.2 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**.

## 27.2.3 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.

## 27.2.4 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**.

## 27.2.5 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**.

## 27.2.6 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**.

## 27.3 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.

### 27.3.1 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**.

### 27.3.2 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** check box.
7. To require each user to enter an electronic signoff when completing the review, select the **Require signoff** check box.
8. Click **OK**.

### 27.3.3 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](#)” on page 571.

2. To view a specific workflow, select the workflow, then select **File > View**.

### 27.3.4 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.
3. Select **Tools > Workflow > Pause Workflow**.
4. If prompted to confirm the pause, click **OK**.

### 27.3.5 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.
3. Select **Tools > Workflow > Resume Workflow**.
4. If prompted to confirm, click **OK**.

### 27.3.6 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**.

### 27.3.7 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.

### 27.3.8 Process a failed task in a workflow

If you are workflow supervisor, and receive notice that an automatic task has failed, you can perform one of the procedures here.

#### To retry a failed automatic task:

1. From your Inbox, open the failed automatic task.
2. Click **Rerun**.
3. Click **OK**.

#### To complete a failed automatic task:

1. From your Inbox, open the failed automatic task.
2. Click **Complete**.
3. Click **OK**.

### 27.3.9 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**.

### 27.3.10 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**.

### 27.3.11 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**.

### 27.3.12 Creating a workflow template

To create a new workflow template, use OpenText™ Documentum™ Content Management Workflow Designer. Use that application's Help for instructions on creating the new workflow template.

## 27.4 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 "[User roles for work queues](#)" on page 576. 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

Administrators create work queues, assign users to work on queue tasks, define the skill profiles that enable the application to assign tasks to the appropriate

processor, and 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 27-1: User roles for work queues**

Role	Description
Queue_processor	Works on items that are assigned by the system from one or more work queue inboxes. Queue processors can request work, suspend, and unsuspend work, complete work, and reassign their work to others.
Queue_advance_processor	Works on items that are assigned by the system from one or more work queue inboxes. Additionally, selects tasks to work on from one or more work queue inboxes.
Queue_manager	Monitors work queues, assigns roles to queues, and assigns users to work on queue items. Queue managers can reassign, and suspend tasks.  Queue managers who have CREATE_GROUP privileges can create work queues.
Queue_admin	Creates work queues, and queue policies. Members of the queue_admin role <i>do not</i> by default have the administrator role.  Queue administrators who have CREATE_GROUP privileges can create work queues.
Process_report_admin	Runs historical workflow reports from the Workflow menu.

#### 27.4.1 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.

## 27.4.2 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.

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.

### 27.4.2.1 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.

### 27.4.2.2 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.

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**.

### 27.4.2.3 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.
3. Under Work Assignment Matching Filters, click **Add**.
4. Select the skills you are adding to work queue.
5. Click the add arrow to move the skills to the content selection area of the page.
6. Click **OK**.

The system prompts you to select the skills for each individual user in the queue.

7. Select the skills for each user, and click **Next**.  
Note that skill profiles are not available for groups.
8. When you have selected the skills for each user, click **Finish**.

**To remove work assignment matching filters from a work queue:**

1. Navigate to the work queue, and select it.
2. Select **View > Properties > Info**.
3. In the Work Assignment Matching Filters table, select the filter that is related to the skills to be changed.
4. Click **Remove**.
5. Click **OK**.

When the system removes the matching filter from work queue, the corresponding skill values set up for users in the work queue are not automatically removed. The skill properties for the user remain until you remove them from the Processor Profile page for each processor.

### 27.4.3 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.

#### 27.4.3.1 Priorities of tasks

For most work queue users, work items appear in the Inbox based on their priority—the highest priority items are assigned to be worked on before lower priority work items. Priority, and aging settings are essential elements in the processing of work queue tasks. When the system creates a new work item, the server identifies the task as a work queue item, and checks for logic to enable it to assign an initial priority to the item. After the task is in the queue, an aging job increases the priority of the task based upon other logic, which moves the task higher in the Inbox until the task is worked on. Priority escalation may trigger the queue administrator to redistribute tasks or reallocate resources between work queues.

The priority level at which a task first appears, and the speed at which it increases in priority can be set either in the work queue policy or in the activity template for the task. For example, you set the initial priority for new tasks in a queue to 1, which means that all new tasks begin with a priority of 1. If you have set the Increment Priority to 10, then whenever the dm\_QmPriorityAging job runs, the priority increases by a factor of ten, if the task has not been worked on. In this example, the task has remained in the queue, and the dm\_QmPriorityAging job has run three times, increasing the priority to 31. The maximum priority field is set to 30, so the system sends a notification to the queue managers group, warning that the task has surpassed its maximum priority, and needs attending to.

Using a work queue policy, the queue administrator or queue manager can specify the initial priority of the task, and the frequency, and percentage at which it increments based on different values you set up in the policy. For more complex initialization, and aging scenarios, you use 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.

#### 27.4.3.1.1 Set dynamic priority and aging logic for tasks

There may be situations where both the initial priority, and the amount that priority increments need to be calculated dynamically. In these cases, you create a *priority module* that the system uses instead of the work queue policy to set priority, and aging logic. A priority module can be selected when creating the work queue policy.

Process data can be used to set the initial priority, and increase the priority based on values in the workflow. For example, if a loan application belonging to a preferred customer comes through a work queue, it can be immediately placed at a higher priority value than a loan application from other customers. In addition, if the loan request is for a greater amount or comes from a preferred loan broker, then the priority can be increased at a higher rate, ensuring that the queue supervisor is alerted if the task is not completed within a specified period of time. This kind of logic can be especially useful to increase the priority of a task as it nears a deadline or some other time restriction—the priority is increased more rapidly as the deadline approaches, pushing the task up the queue at a higher rate.

#### 27.4.3.2 Creating or modifying a queue policy

Each work queue can have one policy. If you associated an override policy with a document being routed in the workflow, the system uses the override policy rather than the work queue policy for that item.

Users with the queue\_admin role can create or modify queue policies.

##### To create or modify a work queue policy:

1. Navigate to **Administration > Work Queue Management > Policies > Work Queue Policies**.
2. Navigate to the category where you want to either locate a new policy or edit an existing one.
3. Do one of these:
  - To create a new policy, select **File > New > Work Queue Policy**.
  - To edit an existing policy, select the policy, and then select **View > Properties > Info**.

You may edit the properties of a policy, but the policy name remains a read-only field. To rename the policy, you must delete the existing policy, and recreate the same policy with the new name.

4. Type a name for the policy.
5. Define these settings:

- **Threshold**

The number of unfinished tasks in the queue at which notifications are sent to the queue manager warning that the number of tasks in the queue is high.

Notifications are triggered when the server runs the dm\_QmThresholdNotification job.

The queue managers group is specified in the queue definition, and defines who receives the notifications.

- **Max Priority**

When a task in the work queue reaches this level, notifications are sent to the queue managers group warning that there is an important task not being processed. Notifications are triggered when the server runs the dm\_QmPriorityNotification job.

- **Initial Priority**

The level of importance that is assigned to a newly created task when the work queue uses this policy. When a task remains in the queue without being worked on, the system adds the number specified in the **Increment Priority** field to this initial number each time the dm\_QmPriorityAging job runs.

- **Increment Priority**

The value by which the system increments the priority level of tasks that are still in the queue each time the system runs the dm\_QmPriorityAging job. It is added to the initial priority each time that the aging job runs.

- **Calculate priorities dynamically**

To use a priority module to set the initial priority, and increase its priority when the aging job runs, select the check box, and choose a priority module from the list-box. *"Set dynamic priority and aging logic for tasks"* on page 581 provides more information on priority modules.

- **Percent Quality Check**

The percent used to randomly decide if the work item must be routed to another processor for a quality assurance check.

6. Click **OK**.

**To delete a work queue policy:**

1. Select the queue policy to delete.
2. Select **File > Delete**.

If the policy is in use, and is referenced by other work queues or work items, the system will not delete the work queue policy.

3. Click **OK**.

## 27.4.4 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.
3. Select **File > Delete**.

The system warns you that this operation cannot be undone.

If the category is in use, and is referenced by other work queues, the system will not delete the work queue category.

4. Click **OK**.

## 27.4.5 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](#)” on page 583, and “[Work queue policies](#)” on page 579 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.

## 27.4.6 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:**

1. Navigate to **Administration > Work Queue Management > Policies > Override Policies**.
2. Do one of these:

- To create a new override policy, select **File > New > Work Queue Override Policy**.
  - To edit an existing override policy, select the override policy, and then select **View > Properties > Info**.
3. If creating a new policy, type a name for the override policy.  
Once the override policy has been saved, the name field becomes read-only.
  4. Click **Add** to view the Work Queue Policy Assignment page, where you can select a work queue, and policy.
  5. Select the queue, and policy names to use as your override policies.
  6. Click **OK**.
  7. To remove a work queue override policy, select it, and click **Remove**.
  8. Click **OK**.

## 27.4.7 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.

### 27.4.7.1 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**.

#### **27.4.7.2 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.

#### **27.4.7.3 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.
4. Under Skills for Work Assignment Matching, click **Add**.
5. Select a filter from the list box.
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.

#### 27.4.7.4 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**.

## 27.4.8 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 Descendents** option enables you to see all work queues that are nested inside of the categories.

Use the **My Categories** link to configure which categories appear in drop-down box of the monitor screen. Only categories that you manage are available for selection.

**To select a work queue category to monitor:**

1. Navigate to **Work Queue Monitor**.
2. Click **My Categories**.
3. Select the categories to monitor. Click the add arrow to move the categories to the content selection area of the page.
4. Click **OK**.

**To view the work queue task a single user or a group is working on:**

Work queue managers, and administrators can view the inboxes of users or groups associated with their work queues.

Users with the queue\_admin or queue\_manager role can perform this procedure.

1. Open **Work Queue Monitor**.  
You can also navigate to **Administration > Work Queue Management**, and select a work queue.
2. Click the queue's *<number>* **users** link in the Active Users column.
3. Select the user or group.
4. Select **Tools > Work Queue Management > Workload**.

The system displays that user's Inbox, and the tasks it contains.

#### To monitor and update active work queues:

1. Do one of these:
  - In the tree pane, click the **Work Queue Monitor** node.
  - Select **Tools > Work Queue Management > Work Queue Monitor**.
2. To view the tasks in the active queue, click either the queue name.  
To view the users in the active queue, click the *<number> users* link (where *<number>* is the number of users).
3. To update queues, see the appropriate procedure.

#### 27.4.8.1 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**.

#### 27.4.8.2 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.
4. Select **Tools > Work Queue Management > Unassign**.

#### 27.4.8.3 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](#)” on page 592.

**To move a task from one queue to another queue:**

1. Click **Work Queue Monitor**.
2. Navigate to the active work queue, and click its name.
3. Select one or more tasks.
4. Select **Tools > Work Queue Management > Move to Queue**.
5. Select the work queue to which to reassign the tasks.
6. Click **OK**.

#### 27.4.8.4 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.
4. Select **Tools > Work Queue Management > Suspend**.



**Tip:** This action is also available through the **Task Manager**.

5. Type the time, and date when you want the application to automatically resume the task.

#### 27.4.8.5 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.
4. Select **Tools > Work Queue Management > Unsuspend**.



**Tip:** This action is also available through the **Task Manager**.

#### 27.4.8.6 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.

## 27.4.9 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.

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.

## 27.5 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.

## 27.6 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 Foundation Java API and directly access the Documentum Client Libraries (DMCL). Therefore, the Foundation Java API cannot perform its usual validation of the methods.

### To run server APIs:

1. Select **Tools > Api Tester**. The API Tester page is displayed.
2. Select **Single-Line Command Entry** or **Script (multi-line) Entry**.
3. Enter the API.
  - If you are in Single-Line mode, enter the command and any necessary data in the **Command** and **Data** text boxes.
  - If you are in Script Entry mode, type the method and its arguments in the **Commands** text box.
4. To display the SQL statement produced by the query, select **Show the SQL**.
5. Click **Execute** to return the results.

## 27.7 Install DAR

The Install DAR page enables you to install the DAR files using Documentum Administrator.

1. Select **Tools > Install Dar**.
2. Browse and select the DAR file you want to install.
3. Click **Install Dar**.



**Note:** The **Install Dar** button is enabled only when you select the correct format of the DAR file.

After the successful installation of the DAR file, a confirmation message appears.

4. Click **Close**.

You can also verify the successful installation of the DAR file using IAPI.



## Chapter 28

# Content Services for SAP Web Administrator

## 28.1 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 Solutions and Content Services for SAP Solutions.

The WebAdmin component to configure and administer Documentum Archive Services for SAP Solutions and Documentum Content Services for SAP Solutions is included in the Documentum Administrator WAR file.

After the successful deployment of Documentum Administrator, you can view the **Content Services for SAP** node in Documentum Administrator.

Install Documentum Archive Services for SAP Solutions and Documentum Content Services for SAP Solutions as described in *OpenText Documentum Archive Services for SAP Solutions - Installation Guide (EDCCOSAPAR-IGD)* and *OpenText Documentum Content Services for SAP Solutions - Installation Guide (EDCCOSAPCS250400-IGD)* respectively.

The **Content Services for SAP** 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 OpenText Documentum CM Queries.
- **SAP:** Defines SAP Queries and configure SAP servers and users for Content Services.

## 28.2 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 Documentum CM Server, it reads the SAP server and user configuration parameters from the repository. The services can be used across multiple SAP application servers.

### 28.2.1 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**.  
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 host name 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`
6. Type the system name and number in the appropriate fields.
7. Click **OK** to save the SAP server configuration.

## 28.2.2 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 Content Services for SAP Solutions WebAdmin, the recommended authorization profiles for SAP users are:

- SAP\_ALL
- SAP\_NEW

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

The **SAP User Properties** page displays.

4. Type the user name in the **New User Name** field.
5. Type the user ID in the **User ID** field.
6. Type a password for the user.

Version 6.0, Content Services for SAP Solutions and later supports case-sensitive passwords when connecting to SAP ECC 6.0 or later. Ensure that the Content Services for SAP Solutions user password you enter exactly matches the SAP user password.

When using Content Services for SAP Solutions 6.0 and later to connect to an older SAP system, the user password entered in Content Services for SAP Solutions must be all uppercase or the kernel patch in SAP note 792850 must be applied to support case-sensitive passwords.

7. Type the client number.
8. Select the language for the user from the **Language** list box.
9. Click **OK** to save the SAP user configuration.

## 28.3 Configuring HTTP Archiving Services

Content Services for SAP Solutions does not include the HTTP archiving services component. Archiving services component has been moved to Archive Services for SAP Solutions. The instructions in this section only apply to environment with parallel installations of Archive Services for SAP Solutions and Content Services for SAP Solutions.

SAP must be configured to work with Content Services for SAP Solutions. *OpenText Documentum Content Services for SAP Solutions - Configuration Guide (EDCCOSAPCS250400-CGD)* provides information about configuring SAP using SAP graphical user interface.

### 28.3.1 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 Documentum CM 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**.  
The **Properties** page displays.
4. Type the archive name in the **Archive Name** field.  
The name can have up to 30 character in length for archives.
5. Type the information on the **Properties** page, as described in the following table:

**Table 28-1: Archive properties**

Field	Description
Archive ID	A two-letter string that specifies the name of the SAP archive.

Field	Description
<b>SAP Document Type</b>	The SAP document type. Select <b>NONE</b> (HTTP provided).
<b>Documentum Type</b>	Specifies the OpenText Documentum CM document type.
<b>Workflow</b>	Specifies a workflow that is associated with the archive. Select <b>No Workflow</b> .
<b>Attribute Map</b>	<p>Specifies the OpenText Documentum CM attributes of an archived document.</p> <p>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.</p>
<b>Filtering</b>	<p>Specifies filters that are applied during archiving. The following filters are available:</p> <ul style="list-style-type: none"> <li>• <b>Custom Filter:</b> 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.</li> <li>• <b>Built-in Filter:</b> Specifies which filters are applied to convert the ALF format into XML for output to PDF, ASCII, or HTML.</li> <li>• <b>Service-based business objects (SBO):</b> Customize archived object behavior.</li> </ul> <p><i>OpenText Documentum Content Services for SAP Solutions - Administration Guide (EDCCOSAPCS250400-AGD) provides more information about filtering.</i></p>

6. Click **OK** to save the archive configuration.

### 28.3.2 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**.  
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.

### 28.3.3 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.
3. Select **File > New > Repository**.  
The **Repository Properties** page displays.
4. Specify 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 repository user.
  - **Domain:** Domain in which the repository resides.Click **Test Connection** to validate the new repository user access credentials.
5. Specify 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.

## 28.4 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 OpenText Documentum CM, providing non-SAP users with searchable access to invoices without having to learn SAP graphical user interface.

There are three parts to the Agent component known as Actions, Agents, and Jobs.

### 28.4.1 Using Auto Manage to execute Content Services for SAP Solutions actions

Agents are used to run an action, such as running a job automatically at regular intervals, monitor job progress and job status.

#### 28.4.1.1 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 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**.  
The **Agent Properties** screen appears.

4. Type a name for the Agent in the **New Agent Name** field.
5. Select the SAP system type from the **SAP System Type** list.
6. Select the action required by the Agent from the **Action** list.
7. Select the SAP server where the Agent is running from the **SAP Server** list.
8. Select the SAP user with the rights to run the Agent from the **SAP User** list.
9. Click **OK** to save the Agent configuration.

### 28.4.1.2 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**.  
The **Register Worker:** page appears.
4. Type a name for the Worker in the **Name** field.
5. Type 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.

### 28.4.1.3 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**.  
The **New Jobscreen** appears with four tabs across the top.
4. In the **Info** tab:
  - a. Type a job name in the **Name** field.
  - b. Type 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**, type 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. Type a title for the system object.
  - b. Type a subject for the system object.
  - c. Click the edit link for **Keywords**, type 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**, type 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**, type 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.

#### 28.4.1.4 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 one 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

*OpenText Documentum Content Management - Server System Object Reference Guide (EDCCS250400-ORD)* provides more information about job status attributes.

## 28.4.2 SAP queries

SAP queries require at least one SAP user and one SAP server.

Queried SAP objects must be linked to a dynamic OpenText Documentum CM 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**.  
The **SAP Query Properties** screen appears.
4. Type the query name in the **Query Name** field.
5. Choose an SAP query type from the **SAP Query Type** list box, as described in [“Query types” on page 610](#).
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 type 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**.
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 28-2: Query types**

Query types for SAP R/3 version 4.6c	Query types for SAP R/3 version 4.7 and 4.6c
Document info record	No Object PLM (Formerly Document info record)
Equipment by short text	Equipment by short text PLM
Functional location by text	Functional location by text PLM
Material by description	<p>Material by description PLM</p> <p> <b>Note:</b> The Material by description PLM query type has three query conditions:</p> <ul style="list-style-type: none"> <li>• MATERIALSHORTDESCSEL_low</li> <li>• MATERIALSHORTDESCSEL_Sign</li> <li>• MATERIALSHORTDESCSEL_Option</li> </ul> <p>All three query conditions are required if the query is to return a result.</p>
Archive data	Archive data
Cost center	Cost center
Financial document	Financial document
Personnel links	Personnel links
Personnel master	Personnel master
Purchasing document	Purchasing document
Customer	Customer Table PLM
Print list	Print list
Vendor	Vendor Table PLM
WBS Element	WBS Element PLM
Asset Master	Asset Master GetList PLM

### 28.4.2.1 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.

#### 28.4.2.1.1 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**.  
The **Documentum Query Properties** screen appears.
4. Type a name for the query in the **Name** field.
5. Type a DQL statement for the query in the **Query** field.

You can use the \$ARG expression when defining the DQL statement. For example:

```
select r_object_id,object_name from dm_document where object_name ='$ARG1'...
```

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.

### 28.4.3 Checking the integrity of linked documents

If links are modified or deleted in SAP directories after SAP and OpenText Documentum CM repository objects have been linked, users do not receive any notifications from Documentum CM 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 OpenText Documentum CM repository and SAP.

**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.
3. Select **File > New > Check Document Info Records**.  
The **Check Document Info Records Properties** page displays.
4. Type 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.

## 28.5 Configuring the Manage and View Components

The Manage component supports Documentum Administrator's certified SAP Messaging Service and PLM interfaces. This functionality requires Desktop Client and OpenText™ Documentum™ Content Management Foundation SOAP API.

### 28.5.1 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**.  
The **Content Services Manage Type Defaults Properties** page displays.
4. Provide the properties information, as described in "[Content Services Manage Type Defaults properties](#)" on page 612.
5. Click **OK** to save the Content Services Manage Type Defaults configuration.

**Table 28-3: Content Services Manage Type Defaults properties**

Field	Description
<b>Document Type</b>	Name of the OpenText Documentum CM object type. Enter dm_document to define default settings for all document types.

Field	Description
<b>SAP Document Type</b>	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.
<b>Description Attribute</b>	Specifies the name of the property that contains the description value. The default value is object_name.
<b>Version Label/Required Version</b>	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.
<b>Status Label/Required Status</b>	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.
<b>Folder path in Docbase/Required Folder</b>	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.
<b>Available Formats/Possible Format</b>	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.
<b>Version Label/Possible Version</b>	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.

## 28.5.2 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**.  
The **Content Services View Properties** page displays.
4. Provide the properties information, as described in “[Content Services View properties](#)” on page 614.
5. Click **OK** to save the Content Services View configuration.

**Table 28-4: Content Services View properties**

Field	Description
<b>Available Formats/Best Formats</b>	Specifies a list of OpenText Documentum CM 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.
<b>Filter Formats</b>	Specifies the formats generated with a Documentum CM 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.
<b>Standard Attributes/Attributes to Display</b>	The attributes that are used as column header in View’s outline view or are displayed upon request in WebView.
<b>Force Login</b>	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.

## Chapter 29

# My Documentum for Microsoft Outlook administration

## 29.1 My Documentum for Microsoft Outlook

My Documentum for Microsoft Outlook is a 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.

After 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.

## 29.2 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.

## 29.3 Profiles

A profile in My Documentum for Microsoft Outlook is a 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.

### 29.3.1 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 **MyDocumentum 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](#)” [on page 617](#).
6. Enter the information on the Target tab, as described in “[The Target tab](#)” [on page 617](#).
7. Enter the information on Import the tab, as described in “[The Import tab](#)” [on page 618](#).
8. Enter the information on the Permissions tab, as described in “[The Permissions tab](#)” [on page 619](#).

### 29.3.2 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 **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.

### 29.3.3 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 right arrow 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.

### 29.3.4 The Import tab

The **Import** tab presents configuration options for importing objects into My Documentum for Microsoft Outlook.

**Table 29-1: Import properties**

Field	Description
<b>Property Inheritance</b>	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.
<b>Provide Dialog Box</b>	Specifies when the user is prompted to complete an import. The options are: <ul style="list-style-type: none"><li>• <i>Always</i>: The user is always prompted to complete the import.</li><li>• <i>Only if a required field is empty</i>: The user is only prompted when at least one of the required fields is empty.</li></ul>
<b>Default settings for Importing Email Messages</b>	Specifies the default message type and permissions set for importing email messages. Select a message type the drop-down list and click <b>Select</b> to select a permission set.  The default message type is dm_document and the default permission set is NONE, meaning the default permissions for that object type are used.
<b>Default settings for Importing Documents</b>	Specifies the default type and permissions set for importing documents. Select a document type the drop-down list and click <b>Select</b> to select a permission set.  The default document type is dm_document and the default permission set is NONE, meaning the default permissions for that object type are used.
<b>Default settings for Importing Folders</b>	Specifies the default type and permissions set for importing folders. Select a folder type the drop-down list and click <b>Select</b> to select a permission set.  The default folder type is dm_folder and the default permission set is NONE, meaning the default permissions for that object type are used.

### 29.3.5 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.

### 29.3.6 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 “Effect of changing availability of My Documentum for Microsoft Outlook profile to disabled” on page 619.

**Table 29-2: Effect of changing availability of My Documentum for Microsoft Outlook profile to disabled**

Client status	Impact
Checked-Out folder contains files	No effect. The client keeps track of checked-out documents and their locations in the repository by unique IDs.
Documents are in import queue	During full synchronization, documents without synchronization jobs are moved to the <b>Lost and Found</b> folder and are not imported. All other synchronization types are no affected.
Items added to the collisions folder during next sync	No effect. The client keeps track of the colliding items and their target locations in the repository by unique IDs.
Any other items	The client discards any other cached documents, even offline-enabled ones, unless they remain accessible through other profiles.

### 29.3.7 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.

## 29.4 Client Setup

On the Client Setup page, an administrator can control the default options that end users can later modify for their client-side installations.

The following table describes the default configuration options for My Documentum for Microsoft Outlook clients.

**Table 29-3: Configuration options for clients**

Field	Description
<b>Automatic Synchronization</b>	Specifies how often and when content is synchronized while a user is connected to the repository. Valid values are: <ul style="list-style-type: none"><li>• <i>Once a day at ...</i>: Content is synchronized once a day at the specified time. The time must be entered in 24 hour format.</li><li>• <i>Once per hour at ...</i>: Content is synchronized once per hour at the specified time. The time must be entered in 24 hour format.</li><li>• <i>Off</i>: Content is not synchronized automatically. The user must manually synchronize the content.</li></ul>

Field	Description
<b>Sessions Kept in History</b>	Specifies the number of synchronization sessions. End users can view the history of previous synchronization sessions. <i>OpenText Documentum My Documentum for Microsoft Outlook User Guide</i> provides more information on setting end-user preferences and viewing synchronization history on an end-user machine.
<b>Maximum Disk Space Allowed</b>	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 <b>Options</b> dialog box in My Documentum for Microsoft Outlook.
<b>Email Address for Support</b>	Specifies the email address for technical requests from end users.

