Administering Content Server

OpenText™ Content Server

This document is part of the Content Server Admin Online Help documentation list. If conflicts exist, the Online Help supersedes this document.

LLESWBA160205-AGD-EN-1

Administering Content Server
OpenText™ Content Server
LLESWBA160205-AGD-EN-1
Rev.: 05. June 2018

This documentation has been created for software version 16.2.5.
It is also valid for subsequent software versions as long as no new document version is shipped with the product or is published at https://knowledge.opentext.com.

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

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

Part 1

Getting Started

Chapter 1

Accessing the Content Server Administration Page

The Content Server Administration page has its own, separate online help content. The online help can help you perform most of the system administration tasks required to maintain Content Server.

The Admin help is not accessible by users who do not have access to sections of the Content Server Administration page. Permission to access some or all of the sections of the Content Server Administration page is granted by either the **Web Admin** usage privilege or by one of the Business Administration usage privileges.

Tip: For information on Business Administration usage privileges, see "Business Administration Usage Privileges" on page 347.

1.1 Understanding the Administration Page

The Administration page is the starting point for most system administration tasks that you perform. This page contains sections with links to other administrative pages. If you install optional modules, links to the module administration pages appear in a new section of the Administration page.

The Administration page is not accessible from the standard user interface. To access the Administration page, users who have sufficient privileges (either the **Web Admin** usage privilege or one of the Business Administration usage privileges) must open a specific URL that ends in `?func=admin.index`. Users who have permission to access the Administration page see an **Admin** menu that contains a link to this URL.

For added security, you can limit access to the Administration page to a list of approved IP addresses. For more information, see "Limiting Admin Account Log-ins by IP Address" on page 87.

You can choose to display the items on the Administration page in a single list view or in a tabbed view.

Changing the Web Administrator Password and the Admin User Password

Some administration pages, such as pages that permit you to manipulate the system's data, prompt you to enter the Web Administration password to gain access.

The Web Administrator password is not the same as the password of the Admin user. The Admin user is a user account created specifically for the Content Server Administrator. It has a bypass privilege that automatically grants full permissions to all items and locations in Content Server without permissions verification.

To change the Web Administrator password, see the **Web Administrator Password** section in “Configuring Basic Server Parameters” on page 73.

To change the password of the Admin user, log on as Admin and click **Change Password** on the **My Account** global menu.

Chapter 2

Administering Permissions

When you set permissions on an item or item type, you specify which users can work on it and what operations those users can perform.

Permissions are nested to indicate dependencies. For example, you cannot have permission to modify a document without having permission to see it. Initially, an item's permission settings are defined by the item's location in Content Server. For example, when you add an item to a folder, the permissions on the folder are applied by default to the new item. You can modify the item's permissions, provided that you have the permission to do so.

Although any user or group can be given the ability to edit permissions, administering appropriate permissions requires a thorough understanding of access control throughout Content Server. Before you begin creating users and groups, OpenText recommends that you carefully review the following information about permissions: “Choosing Types of Permissions” on page 12, “Copying, Mapping, and Deferring To Permissions” on page 15, and “Strategies for Administering Permissions” on page 16.

2.1 Setting User Tab Permissions

You can set permissions for users to modify user information tabs. Users can have the Edit Self or Edit Anyone privileges for either the **General** tab or the **Personal** tab. By default, users with the System Administration Rights privilege also receive full Edit Anyone privileges. You can grant other users the Edit Anyone privilege for the Personal tab, but not the General tab. You can set all users to have the Edit Self privilege for either or both tabs.

2.1.1 To Set User Tab Permissions

To set User Tab Permissions:

1. On the **Administration** page, select **Users and Groups Administration**.
2. Select **User Tab Permissions**.
3. To modify the privileges for all users, do the following:
    - Click the **<Public Access>** link.
    - Select or clear the **Allow Edit of Self** check box for each tab.
    - Click the **Update** button.
4. To allow a new user or group to have Edit Anyone privileges, do the following:
    - Click the **Grant Access** icon ⊕.

- Find the user or group to which you want to grant access.
- Select the **Grant Access** check box.
- Click the **Submit** button.
- Select the **Allow Edit of Anyone** check box for each tab you want available.
- Click the **Update** button.

5. Click the **Done** button.

2.2 Choosing Types of Permissions

Permissions specify which users or groups can operate on an item and which operations those users or groups can perform. The Admin user always has full access to all items in Content Server. By default, individual users also have full access to all items in their own Personal Workspace. For more information on this topic, see *OpenText Content Server - Get Started (LLESRT-UGD)*.

There are three distinct but related types of permissions:

- Work Item permissions, which apply to Channels, Discussions, and Task Lists.
- Document Management permissions, which apply to most item types.
- Role-Based permissions, which apply to Projects.

For more information on this topic, see *OpenText Content Server - Get Started (LLESRT-UGD)*.

2.3 Understanding Document Management Permissions

Document management permissions apply to document management items, such as documents, folders, compound documents, workflow maps, URLs, aliases, and generations. Document management permissions are more detailed than work item permissions and provide more precise control over the operations performed on document management items.

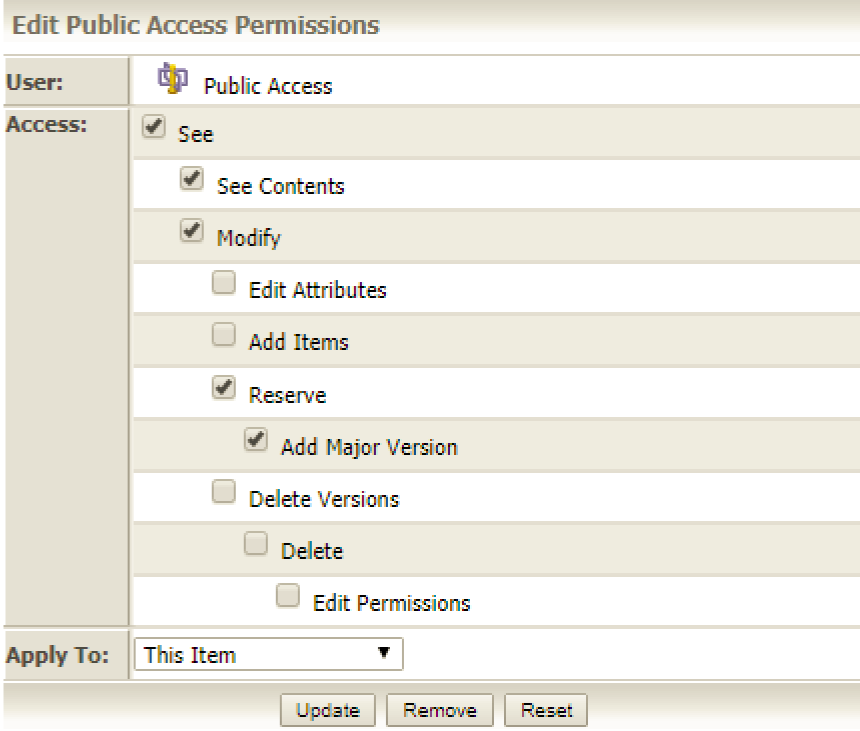
The following list describes the document management permissions:

- **See** - The user or group can view the item name.
- **See Contents** - The user or group can view the item name and open the item.
- **Modify** - The user or group can rename the item and modify some of its properties (for container items, such as folders, this includes the properties that are listed on the item's Presentation Info page).
- **Edit Attributes** - The user or group can assign a category to an item, modify an item's custom attributes, or modify its category.

- **Add Items** - The user or group can add items to the item. The **Add Items** permission is only available for items that can contain other items, such as folders and compound documents.
- **Reserve** - The user or group can reserve the item, modify it, and then unreserve the item. The user can also add versions to items. If a Document uses advanced versioning, the user can add minor Versions of the Document˙. The **Reserve** permission is only available for items that can be reserved, such as documents and workflow maps.
- **Add Major Version** - The user or group can add a Document as a major Version or promote a minor Document Version to a major Version. This permission only applies to Documents that use advanced versioning.
- **Delete Versions** - The user or group can delete versions of the item, and delete minor Versions of Documents that use advanced versioning. The **Delete Versions** permission is only available for items that have versions, such as documents and workflow maps.
- **Delete** - The user or group can delete the item, and delete major Versions of items that use advanced versioning.
- **Edit Permissions** - The user or group can change the permissions that other users or groups have on the item, and can modify the **Version Control** settings of a Folder.

When you select a document management permission, Content Server verifies that the base set of dependent permissions required for that permission are also selected. All permissions contain the **See** permission, for example. Users and groups cannot have permission to modify, add, delete, or reserve an item unless they first have the **See** permission. Similarly, the **Edit Attributes**, **Reserve**, **Add Items**, and **Delete Versions** permissions contain the **Modify** permission. **Delete** and **Edit Permissions** contain the **Delete Versions** permission.

Note: The **Delete Versions** and **Reserve** permissions do not apply directly to folders or compound documents. These permissions are available in the permissions set for compound documents and folders primarily so that you can specify default permissions for items that are added to the folder or compound document.



Edit Public Access Permissions

User: Public Access

Access:

- ☑ See
  - ☑ See Contents
  - ☑ Modify
    - □ Edit Attributes
    - □ Add Items
    - ☑ Reserve
      - ☑ Add Major Version
    - □ Delete Versions
      - □ Delete
        - □ Edit Permissions

Apply To: This Item

Content Server automatically enables permissions that are contained within any permission that you select. For example, in the image above, if you select the **Add Major Version** check box when no other permissions are selected, Content Server automatically selects the **Reserve**, **Modify**, **See Contents**, and **See** check boxes.

2.4 Understanding Role-Based Permissions

Projects simplify the definition of access control by providing a role-based permissions model. When you create a Project, Content Server automatically creates a Coordinator, Member, and Guest group for the Project. Each of these groups is assigned a Project role and therefore receives a different level of permissions.

The following list describes the different Project roles and the permissions associated with it:

- **Guest** – users who are made guests of a Project can open the items contained in the Project.
- **Member** – Project members can open and modify the items contained in the Project. Members can also add items, edit attributes, add and delete versions, and reserve items contained in the Project. Members can also delete the items they create or add to the Project.
- **Coordinator** – In addition to the Guest and Member permissions, Coordinators can establish access privileges, define permissions, add or remove participants, and change a participant's role within the Project.

Adding Projects to Folders

When you add a Project to a folder, users and groups who have access to the folder become participants in the Project. In addition, the folder's permissions are mapped to the three types of Project roles. The type of permissions that a user or group has for a folder determines whether they become Guests, Members, or Coordinators of any new Project added to that folder. Permissions are mapped in the following manner:

- Users or groups with **See** and **See Contents** permissions on the folder become Guests of the Project.
- Users or groups with **See**, **See Contents**, and **Add Items** permissions on the folder become Members of the Project.
- Users or groups with **Modify**, **Edit Attributes**, **Delete Versions**, and **Reserve** permissions on the folder (in addition to **See**, **See Contents**, and **Add Items** permissions) also become Members of the Project.
- Users or groups with all permissions on the folder become Coordinators of the Project.

By default, when you add an item to a Project you can modify the permissions assigned to that item. However, you cannot reduce the permissions for a Coordinator of a Project. Coordinators always have full access to all items in the Project.

To expand or reduce the access for certain Guests or Members of a Project, a Coordinator of a Project can edit their permissions on items in the Project Workspace. Coordinators can also change the roles of participants in a Project.

Members of a Project can create a subproject by adding a Project within the parent Project. In this case, Coordinator, Member, and Guest groups are initially copied to the subproject. The creator of the subproject can expand or reduce the access for certain Guests or Members of the parent Project, but cannot remove Coordinators of the parent Project from the subproject's Coordinator group.

2.5 Copying, Mapping, and Deferring To Permissions

Content Server items establish permissions by copying or mapping permissions from other items or by deferring to the permissions of other items. For example, items that you add to a folder or compound document automatically inherit the same permissions assigned to the folder or compound document. Items that you add to a Channel, Discussion, or Task List defer to the permissions assigned to the Channel, Discussion, or Task List in which they reside. Content Server items that contain other items are called *parent* items and the items that they contain are called *child* items.

Permissions are automatically assigned to items when they are added, copied, or moved in Content Server and when you apply them to subitems. Permissions are mapped from one item to another when you add work items or Projects to folders or compound documents. Permissions are also mapped when you add document management items, such as documents, folders, compound documents, workflow maps, URLs, aliases, and generations, to Projects.

2.6 Applying Permissions to Subitems

Although some items copy their permissions from their *parent* items, the items in which they are contained, you can overwrite those permissions to customize the access control for particular items. Another way of overwriting permissions is to apply the permissions that you set for a container to all of the items stored inside it.

When you click the **Apply To subitems** button on the Permissions page for a container, Content Server applies the container's permissions to all items below it in the hierarchy. For example, if you change a folder's permissions and you want to apply the new permissions to the contents of the folder, you can click the **Apply To subitems** button. When you apply the current item's permissions to all subitems in the hierarchy, you overwrite any customized permissions previously applied to the subitems. After you click the **Apply To subitems** button, a message indicates the number of items that were affected.

If you do not have the Edit Permissions permission for certain items in the hierarchy, the permissions for those items are not affected when you click the **Apply To subitems** button. Use the **Apply To subitems** button with caution, however, because it overwrites other permissions in the hierarchy. If you grant more access to items high in the hierarchy and then apply your changes to all subitems, you could unintentionally open up access on a restricted item. For more information about the **Apply To subitems** button, see “Strategies for Administering Permissions” on page 16.

If you click the **Apply To subitems** button in a folder that contains Projects, subprojects, task lists, Channels, or Discussions, the folder's permissions do not take effect. That is because the permissions for these items are protected.

2.7 Strategies for Administering Permissions

Understanding access control and administering permissions lets you create a secure, organized environment for the users and groups in Content Server. Although Content Server defines the rules for assigning permissions for you, the way that you assign permissions to the items depends on the knowledge management strategy that you adopt. You can administer permissions, establish Knowledge Managers to administer permissions for you, or trust users and groups to administer permissions individually. The strategy that you choose depends on your organization and its knowledge management needs. Although there is no single solution, there are some strategies that can help you work more efficiently.

1. *Establish Knowledge Managers for the primary containers in the Enterprise Workspace.*

   Knowledge managers are users or groups who have ownership and administrative responsibilities for items. They are responsible for administering permissions and monitoring activity. Consider appointing Knowledge Managers and letting them administer key areas, assign permissions, and manage the content of the folders and containers in those areas.

- Specifying Knowledge Managers as the Owner Group for a container and opening up their permissions—while restricting the permissions of other users and groups—grants them primary ownership of key areas.
- Allowing Knowledge Managers to edit the permissions of a container item is an effective way to regulate access control for primary areas.

2. *Define the Personal Workspace.*

   Defining the purpose of Personal Workspaces ensures that all users and groups follow the strategy that you outline. You can let individual users determine the permissions for their Personal Workspaces based on that strategy.

   - Using Personal Workspaces as storage areas for works in progress is an effective way of backing-up data.
   - Using Personal Workspaces as storage areas for sensitive items lets you maintain control over the content of items while granting access as needed.
   - Creating aliases lets you share items in your Personal Workspace with other users and groups in the Enterprise Workspace.

3. *Segregate sensitive items.*

   Identify sensitive items and segregate them from less sensitive items. Sensitive items include private documents, Discussions, Projects, or other items for which security is especially important.

   - Moving sensitive items to a separate folder lets you administer strict permissions to all related items without restricting access to less sensitive items.
   - Creating aliases to sensitive items in less sensitive folders lets you group related items while retaining access permissions.

4. *Create Projects.*

   Create Projects for simpler access control. Projects offer a default set of permissions that are clearly defined and easy to understand.

   - Creating Projects lets you administer permissions using a simple, role-based permissions model.
   - Editing the ACL and Project roles for participants within a Project lets you expand or restrict permissions.

5. *Avoid applying Permissions to subitems.*

   Beware of the **Apply To subitems** button—especially when opening up permissions at the top of a hierarchy.

   - Applying permissions to all subitems copies the entire ACL to all items below the current item in the hierarchy.
   - Logging in as a user other than Admin can limit your permissions and prevent you from making changes to all permissions in a hierarchy using the **Apply To subitems** button.

- Notifying Knowledge Managers and other interested users or groups after applying permissions to subitems lets them readjust their custom permission settings, if necessary.

Part 2

Server Configuration

Chapter 3

Configuring General Environment Settings

Configuring the appearance and behavior of your Content Server system includes the following tasks:

Some related settings are administered elsewhere in the Administration interface. For information about configuring user password options and the user name display, see “Configuring User Settings” on page 427. For information about configuring global user interface preferences, such as the default start page that appears when users log in to Content Server, see “Configuring Basic Server Parameters” on page 73. For setting Date and Time Formats, see “Setting Date and Time Formats” on page 30.

3.1 Editing the Enterprise Menu

You can add URLs to the Enterprise menu quickly and easily from the Administration page. A URL that you add can be to any webpage that Content Server can access using the HTTP protocol, either on the Internet, on your organization's intranet, or within Content Server itself. The added items appear beneath a separator under the default Enterprise menu items.

3.1.1 To Edit the Enterprise Menu

To add an item to the Enterprise menu:

1. Click the **Additional Enterprise Menu Items** link in the **Server Configuration** section on the Administration page.
2. In the **Name** field, type the name of the item. This is the text that you want to display in the Enterprise menu.
3. Type a URL in the **URL** field.
4. Click **Add Menu Item**.
5. Click the ⇧ and ⇩ buttons to move the item either up or down in the menu order.
6. Click **Submit**.
7. Restart Content Server.

Note: Click the ⊟ button to remove the selected item from the **Enterprise** menu.

3.2 Configuring Features

The **Configure Features** administration page provides access to the **Configure Container Options** and **Configure Thumbnails** administration pages. These are two of the pages that are available to a user with the "The Available Features Usage Privilege" on page 349, which is one of the "Business Administration Usage Privileges" on page 347.

3.2.1 Configuring Container Options

The **Configure Container Options** page has settings that control the appearance of Content Server containers: whether they have a hyperlink trail or drop-down list, how long the **New** and **Modified** indicators appear, and whether Content Server displays the total number of items in a Container. Other settings on the **Configure Container Options** page affect how users interact with Content Server containers. You can configure pagination, filtering, and column customization, set the behavior of featured items and Custom Views, set the maximum numbers of items that can appear on a single Edit/Organize page, and enable drag and drop in the Content Server Classic View. Users can be allowed to select their own folder icons or not.

Navigation

You can specify a navigation style, which determines how Content Server displays the path to the current item or location, as a list or as a hyperlink trail. You can also allow users to change the navigation style, if they prefer.

To allow users to access Content Server *Smart View* interface, select **Enable Smart View Link**. When this option is selected, and users are within a container that is accessible through both the Classic View and the Smart View, a **Smart View** option appears on the **My Account** menu that allows users to open the current container in the Smart View.

Duration of "New" and "Modified" Indicators

These settings specify the number of days that the **New** or **Modified** icons appear beside items. By default, the **New** icon appears for two days after an item is added, and the **Modified** icon appears for seven days after an item is changed.

Size Display

Selecting **Hide Number of Items** in the **Container Size Display** row prevents Content Server from showing users the number of items that are in a container.

Note: This setting affects Prospectors as well. Prospector nodes display an empty size value when this parameter is set.

Pagination

When pagination is enabled, Content Server displays large numbers of items over a series of pages, instead of all on one page. Enabling pagination makes it easier to browse Folders and Workspaces that contain numerous items.

Pagination is enabled by default. Disable pagination if you want users to always see all of a container’s contents on a single page.

If pagination is enabled, you can specify the choices that users have for the number of items that appear on each page in a Content Server container by entering values for the **Number of Items Shown Per Page** menu and selecting one of those values as the **Default Number of Items Shown Per Page**. If the number of items in a container is larger than the number selected by the user, Content Server displays the contents of the container over multiple pages, and provides controls for browsing the pages. If the number of items in a container is smaller than the number specified, Content Server displays the contents of the container on a single page, and the arrows for browsing to previous and subsequent pages do not appear.

The **Store page information in cookie** option causes Content Server to remember the page number that you are currently viewing. When you open the same container in another browser tab or window, Content Server places you on the same page. If the option is cleared, when you open a new tab or window, Content Server places you on the first page.

If your Content Server deployment includes folders that contain so many child items that browsing performance is affected, you can use the **Maximum Viewable Items** setting to improve performance and user experience. If you enable this setting, users cannot browse folders that contain more direct child items (not counting items in subcontainers) than the value of **Maximum Viewable Items**. This does not mean that the folder’s contents are inaccessible. Users can still access their contents by searching or using any of the available facets on the **Content Filter** sidebar.

Note: Pagination must be enabled before you can enable the **Maximum Viewable Items** setting.

The exact effect of this setting depends on your current view. If you attempt to browse a folder that contains more than the Maximum Viewable Items:

- in the Smart View, Content Server displays **Browse has been restricted as there are too many items**.
- In the Classic View, Content Server either allows limited browsing (the default option) or prevents browsing altogether, depending on the value of **Allow users to add items or browse sub-containers, even if the threshold is reached (Classic UI only)**.

By default, **Allow users to add items or browse sub-containers, even if the threshold is reached (Classic UI only)** is enabled and limited browsing is permitted. Users in the Classic View can browse into a folder that contains more than the **Maximum Viewable Items** and can see subfolders and other containers within the folder, but not Documents and other individual items. If this setting is disabled, such folders are not clickable and users cannot even attempt to open them.

Configure Edit/Organize

Specifies the maximum number of items that Content Server displays on a single Edit/Organize page. (The limitation applies only to Edit/Organize pages, for example the **My Favorites** and **My Projects** pages, not standard browse pages.) By default, the maximum is 100 items per page. When the **Maximum Items Per Page** is exceeded, Content Server splits the Edit/Organize page into multiple pages. The limit then applies to each split page individually.

Column Customization

When column customization is enabled, users can customize the way that columns are displayed in a browse list. By default, column customization is disabled.

Featured Items

When **Remove Featured Items from Browse List** is enabled, featured items do not appear in the browse list. By default, featured items do appear in the browse list.

Filtering

When filtering is enabled, Content Server displays boxes at the top of the browse view that allow users to filter by item type or by item name. Enabling filtering makes it easier to find items inside a container that contains a large number of items. Filtering is enabled by default.

Note: The **Content Filter** sidebar and filtering are mutually exclusive. When both the sidebar and filtering are enabled, filtering is available only on containers that do not display the sidebar. For information on the sidebar, see "Configuring the Sidebar" on page 40.

Administrators can enable and disable filtering for containers in Content Server. When filtering is disabled, the **Filter by name** and **Filter by Item Type** boxes do not appear in Content Server containers.

The following two settings affect what happens when a user applies filtering to a container and then opens that same container in another browser tab or window:

Store item filter information in cookie
This setting causes Content Server to remember the item type that you filter by. When you open the same container in another browser tab or window, it remains filtered by item type. If you clear this option, Content Server displays all item types by default when users open a new page or tab.

Store name filter information in cookie
This setting causes Content Server to remember the name that you filter by. When you open the same container in another browser tab or window, it

remains filtered by item type. If you clear this option, Content Server does not filter by name when you open the same container in a new page or tab.

Drag and Drop

In this section, you can enable or disable drag and drop in the Content Server Classic View. By default, Drag and Drop is enabled.

Note: The settings in this section affect drag and drop operations in the Content Server Classic View. They do not affect the behavior of the Smart View.

You can also configure the following related settings:

Enable Logging to Browser Console
Produces detailed logging on Drag and Drop operations. This can be a useful setting if you need to troubleshoot a problem with Drag and Drop.

> **Important**
> OpenText recommends that you do not enable logging to the browser console except at the request of OpenText Technical Support.

Add Version
What Content Server does when a user drags and drops an item into a folder that already has an item with the same name (adds a version of the item or skips the upload).

Maximum Number of Files Allowed In A Drop
The maximum number of files that you can drag and drop in a single operation.

Maximum File Size For A Drag and Dropped File (MB)
The maximum size of a file that you can drag and drop into Content Server.

> **Note:** OpenText recommends that you set the **Maximum File Size For A Drag and Dropped File (MB)** to the maximum upload value permitted by your web server. You can set it to a larger value, but if you attempt to upload a file that is larger than the maximum upload value permitted by your web server, the operation will fail.

Custom View File Listing

This setting determines the way that Content Server displays a folder that contains only a hidden Custom View. If the folder contains any other items, this setting has no effect.

If **Show File Listing** is cleared (the default option), Content Server displays only the contents of the hidden Custom View. It does not show the file listing that appears on a normal browse view page and it does not show the Content Filter Sidebar.

If **Show File Listing** is selected, Content Server displays the contents of the Custom View and the normal browse view, including the Content Filter Sidebar if the current user has enabled it. Because the folder contains no items other than a hidden Custom View, no items are listed in the browse view. Instead the message **There are no items to display** appears.

Note: This setting does not apply to virtual folders.

Administer Icons For Folders

Enabling this parameter allows users to select additional icons for Content Server folders. This parameter is disabled by default.

To Configure Container Options

To configure container options:

1. On the Content Server Administration page, under **Server Configuration**, click **Configure Features**.

2. On the **Configure Features** page, click **Configure Container Options**.

3. On the **Configure Container Options** page, in the **Navigation** section:

   a. In the **Navigation Style** field, select either **Hyperlinked Trail** to select the hyperlink view, or **Drop-Down List** to select the drop-down list view.

   b. Optional In the **Allow user to override** field, to prevent users from altering their personal navigation style, clear the box. It is enabled by default.

   c. Optional In the **Browse Appearances** field, to include Appearances in the Target Browse dialog box, select the box. It is disabled by default.

   d. Optional In the **Enable Smart View Link** field, select **Enable Smart View Link** to allow users to switch to the Smart View from the Classic View. This option, when enabled, appears on the **My Account** menu. It is only available to users when the container is accessible in both views.

4. In the **Size Display** section:

   - Optional In the **Container Size Display** box, select **Hide Number of Items** to prevent the number of items in a container from being displayed.

5. In the **Pagination** section:

   a. Optional Clear **Enable Pagination** to disable pagination. Pagination is enabled by default.

   b. Optional In the **Number of Items Shown Per Page** box, type a list of positive integers. These numbers will become the choices that users can select for the number of items that they want Content Server to display per page.

   c. Optional From the **Default Number of Items Shown Per Page** menu, select the number of items that will appear on each page by default. The choices in the menu are determined by the numbers in the **Number of Items Shown Per Page** setting.

   d. Optional Pagination settings are stored in a cookie by default. If you do not want to store pagination settings in a cookie, clear **Store page information in cookie**.
   e. Optional To prevent browsing of containers with large numbers of items, select **Prevent browsing of containers that exceed the Maximum Viewable Items** and specify a value for **Maximum Viewable Items.** To allow users to browse subfolders in affected containers in the Classic View, select **Allow users to add items or browse sub-containers, even if the threshold is reached (Classic UI only)**.

6. Optional Column customization is disabled by default. To permit users to customize the columns displayed in a browse list, select **Allow Browse List Column Customization**.

7. Optional Featured items appear in the browse list by default. To remove featured items from the list view, select **Remove Featured Items from Browse List**.

8. In the **Filtering** section:

   a. Optional Filtering is enabled by default. To disable filtering, clear the **Enable Filtering** box.
   b. Optional If you do not want item filter information stored in a cookie, clear **Store item filter information in cookie**. Item filter information is stored in a cookie by default.
   c. Optional If you do not want name filter information stored in a cookie, clear **Store name filter information in cookie**. Name filter information is stored in a cookie by default.

9. In the **Drag and Drop** section:

   a. Optional If you want to disable Drag and Drop, select the **Enable Drag and Drop** box. Drag and Drop is enabled by default.
   b. Ensure that the **Enable Logging to Browser Console** box is cleared unless OpenText Technical Support has requested that you enable this setting. Logging to browser console is disabled by default.
   c. In the **Add Version** field, select one of:

      - **Add a version if file exists**
      - **Skip file if file already exists**
   d. In the **Maximum Number of Files Allowed In A Drop** field, enter a positive integer. The default is 500.
   e. In the **Maximum File Size For A Drag and Dropped File (MB)** field, enter a positive integer. The value should not exceed your webserver's maximum value. The default is 100.

10. Optional If you want to show the file listing if the container has a hidden Custom View, select **Show File Listing**. The file listing is hidden by default.

11. Click **Save Changes** to save your changes and return to the previous screen, or click **Reset** to reset the page to its previous values.

3.2.2 Configuring Thumbnail Options

You can specify whether thumbnails are generated when Content Server indexes documents in an Enterprise Data Source.

If users add documents to Content Server when the **Generate Thumbnails** setting is enabled, the Document Conversion process automatically generates thumbnails of the first page of each document during indexing.

During the indexing process, the thumbnails are first stored in a temporary directory on each Admin server that runs the Document Conversion process within an Enterprise data flow. During system object test runs, the Content Server agent that tests the objects retrieves the thumbnails, deletes them from the temporary directory, and adds them to Content Server. The thumbnails are then displayed on the document **Overview** and **Search Results** pages, and in the **Featured Items** sections. For more information about data flow processes, see *OpenText Content Server - Administering Search (LLESWBS-AGD)*.

You can generate thumbnails for either the current versions of documents or for all versions, and specify which MIME types to generate thumbnails for.

If users add documents to Content Server when the **Generate Thumbnails** setting is disabled, no thumbnails are generated. Instead, large icons are displayed for the documents in the user interface.

Note: The **Generate Thumbnails** setting is enabled by default.

Supported MIME Types

You can generate thumbnails during Document Conversion for specific types of documents, based on analysis of the document. The **Configure Thumbnail Options** page defines to the Extractor which Content Server MIME types are candidates for thumbnail generation. Defining thumbnails on this page will only produce thumbnails if the file format is supported, and the MIME type is defined in the `[Thumbnail]` section of the `dcsrules.txt` file.

The following file formats can be configured to generate thumbnails in the Document Conversion server:

- Word 95-2013
- Excel 95-2013
- PowerPoint 97-2013
- PDF 1.0 – 1.9
- DWG
- DWF
- CADRA
- WordPerfect
- Postscript
- Micro Station (DGN)
- RDL
- RTF
- Calcomp
- HPGL
- DXF
- Gerber
- CGM
- EMF
- WMF
- ME10
- JPEG
- BMP
- PNG
- GIF
- TIF
- CALS

To Configure Thumbnail Options

To configure Thumbnail Options:

1. On the Content Server Administration page, under **Server Configuration**, click **Configure Features**.
2. On the **Configure Features** page, click **Configure Thumbnails**.
3. On the **Configure Thumbnail Options** page, click the **Enable** radio button for **Generate Thumbnails**.
4. For **Thumbnail Versions**, click the **Current version only** radio button to generate thumbnails for the current version of the object only, or click the **All versions** radio button.
5. For **MIME Types**, click the **edit / review list** link to open the **Configure Thumbnail MIME Types** page. For details, see "To configure the MIME types for generating thumbnails:" on page 29 and "Supported MIME Types" on page 28.

   Note: Thumbnails are generated during indexing. The thumbnail MIME types act as an indexing white list, and take precedence over the Extractor MIME type exclusion list in the `[ExcludedMimeTypes]` section of the `opentext.ini` file.

   For thumbnail generation to work, the MIME type must be selected on the **Configure Thumbnail MIME Types** page, and the MIME type needs to be defined in the `[Thumbnail]` section of the `dcsrules.txt` file.

6. For **Display Thumbnails**, click the **Enable** radio button to display thumbnails instead of large icons.
7. Click **Save Changes**.

To configure the MIME types for generating thumbnails:

1. On the Content Server Administration page, under **Server Configuration**, click the **Configure Thumbnails** link.
2. On the **Configure Thumbnail Options** page, for **MIME Types**, click the **edit / review list** link to open the **Configure Thumbnail MIME Types** page.
3. On the **Configure Thumbnail MIME Types** page, select the check boxes for the MIME Types to extract to the search index. See "Supported MIME Types" on page 28 for more information.
4. Click **Update**.

3.3 Setting Date and Time Formats

You can configure the time and date formats so that they conform to the standard formats used at your organization. If more than one language is enabled, the date and time formats can be configured individually for each language. You can specify formats for the following date settings:

- **Time Zone**, which lets you set Content Server to automatically calculate and display the correct time in each user's local time zone. By default, Content Server displays the local time at the server's location
- **Input Date**, which specifies how users must enter dates and times when prompted for this information by Content Server.
- **Short Display Date**, which controls how Content Server displays short-format dates. This format includes the day of the week, which precedes the date display.
- **Long Display Date**, which governs how Content Server displays long-format dates.

By default, all three date settings are the same: `month/day/year`, with a two-digit month, a four-digit year, a 12-hour clock, and the slash (/) as the separator.

3.3.1 To Set Date and Time Formats

To set date and time formats:

1. In the Administration page, under either **Server Configuration** or **Languages**, click the **Administer Date/Time** link.
2. In the **Time Zone Configuration** section, to override the server time, click the **Enable Time Zone Offset** check box.
3. In the **Input Date Format** section, do the following:
   - In the **Date Order** drop-down list, select the order in which you want input fields to appear for the day, month, and year. The default setting at install is MM/DD/YYYY. Any change you make will display in the **Example** field below.
   - Select the **Two-part Year** check box to have two drop-down lists for year inputs. One list will refer to the century, 19 and 20. One list will refer to the decade, 00 through 99. The default setting for this check box is unchecked.
   - Select the **24-Hour Clock** check box to display times in the 24-hour clock format, for example, `14:41`. The default setting displays the time in 12-hour AM/PM format, for example, `02:41 PM`. Any change you make will display in the **Example** field below.
4. In the **Short Display Date Format** section, do the following:
   - In the **Date Order** drop-down list, select the order in which you want display fields to appear for the day, month, and year. The default setting at

install is MM/DD/YYYY. Any change you make will display in the **Example** field below.

- Select the **Two-Digit Year** check box to display years as two-digit numbers, for example, `09` to represent 2009. The default setting at install will display the year as a four-digit number, for example, `2009` to represent 2009. Any change you make will display in the **Example** field below.
- Type the characters that you want to use to separate the elements of the date in the **Date Separators** fields. In the first field, type the character that you want to use between the first and second elements. In the second field, type the character that you want to use between the second and third elements. The default setting at install will use the forward slash character, `/`, as separators. Any change you make will display in the **Example** field below.

5. In the **Long Display Date Format** section, do the following:

   - In the **Date Order** drop-down list, select the order in which you want display fields to appear for the day, month, and year. The default setting at install is MM/DD/YYYY. Any change you make will display in the **Example** field below.
   - Select the **Two-Digit Year** check box to display years as two-digit numbers, for example, `09` to represent 2009. The default setting at install will display the year as a four-digit number, for example, `2009` to represent 2009. Any change you make will display in the **Example** field below.
   - Type the characters that you want to use to separate the elements of the date in the **Date Separators** fields. In the first field, type the character that you want to use between the first and second elements. In the second field, type the character that you want to use between the second and third elements. The default setting at install will use the forward slash character, `/`, as separators. Any change you make will display in the **Example** field below.
   - Select the **24-Hour Clock** check box to display times in the 24-hour clock format, for example, `14:41`. The default setting displays the time in 12-hour AM/PM format, for example, `02:41 PM`. Any change you make will display in the **Example** field below.

6. To save your changes, click **OK**. On the **Restart Content Server** page, click **Restart** to restart Content Server automatically, or click **Continue** if you prefer to use the operating system to restart Content Server.

3.4 Configuring the Functions Menu

On the Configure Function Menu page, you can determine where functions appear on the **Functions** Menu for every item. You decide whether an item's function appears in the main part of the **Functions** menu or hidden from users in the **More** submenu. Item functions are categorized based on their similarities, with the most common functions appearing at the top of the menu.

For example, opening, downloading, or viewing a Document as a webpage are similar concepts and are grouped together.

The following list describes the different types of functions:

- **Group 1 GET IT**, which allows the user to retrieve the item or its data.
- **Group 2 AFFECT ITS CONTENT**, which allows the user to change an aspect of the item.
- **Group 3 AFFECT ITS LOCATION**, which allows the user to copy, move, or create an item from another item.
- **Group 4 TRACK IT**, which informs the user that something happened to the item.
- **Group 5 COMMUNICATE ABOUT IT**, which allows the user to inform other users about the item.
- **Group 6 AFFECT ACCESS**, which allows the user to control or permit access to items.
- **Group 7 SUB AREAS**, which allows the user to access module functionality.
- **Group 8 STILL LOOKING**, which allows the user to find similar items.
- **Group 9 REMOVE IT**, which allows the user to delete items.
- **Group 10 DETAILS**, which allows the user to view, delete, or change item information.

Notes

- Whether item functions appear in the main menu or the **More** submenu, standard item permissions only allow users to see functions for which they have permission.
- If your Content Server installation has been upgraded from Content Server 9.7.1 and your environment includes modifications to the **More** Functions menu item, it is possible that the **More** Functions menu item does not appear for some or all of your users. This is most likely to happen to users who access Content Server in a language other than English. To resolve this problem, open the **Configure Functions Menu** administration page and, without making any changes to your Functions menu configuration, click **Save Changes**.

3.4.1 To Configure the Functions Menu

To configure the Functions menu:

1. In the **Server Configuration** section on the Administration page, click the **Configure Function Menu** link.
2. On the Configure Function Menu page, click one of the following radio buttons for each function:
   - **Main**, which displays the function in the main section of the **Functions** menu.
   - **More**, which displays the function in the hidden section of the **Functions** menu.
3. Click the **Save Changes** button.

Note: If your Content Server installation has been upgraded from Content Server 9.7.1 and your environment includes modifications to the **More** Functions menu item, it is possible that the **More** Functions menu item does not appear for some or all of your users. This is most likely to happen to users who access Content Server in a language other than English. To resolve this problem, open the **Configure Functions Menu** administration page and, without making any changes to your Functions menu configuration, click **Save Changes**.

3.5 Configuring Log Settings

On the **Configure Log Settings** page, you can enable and disable Content Server logging, specify log levels, and make other log configuration settings. Changes made on this page apply to the current Content Server instance. If you have a clustered deployment of Content Server, you should configure logging for each Content Server instance separately.

Important

To enable logging for a remote computer running the Secure Enterprise Access (SEA) servlet, you must edit the settings directly in the `opentext.ini` file of that Content Server instance. For more information, see the following topics

- “[cgi_logs]” on page 99
- “[connect_logs]” on page 104
- “[receiver_logs]” on page 198
- “[socketServer_logs]” on page 211
- “[thread_logs]” on page 219
- “[timing_logs]” on page 221

On the **Configure Log Settings** page:

- You can enable and configure the following log types

  Thread logs
  If Thread logs are enabled, Content Server generates a Thread log file for each of its threads and continuously updates it to record the data that it sends on the thread.

  SQL Connect logs
  If SQL Connect logs are enabled, Content Server generates a SQL Connect log file for each of its threads. SQL Connect logs contain information, including SQL statements, on the communications between Content Server and the Content Server database.

  Web Server Client logs
  If Web Server Client logs are enabled, a file is generated each time a user's Web browser sends Content Server a request. The name of the file depends on the request handler.

  - For CGI, the file name is `llclient`*<###>*`.out`.
  - For `llisapi.dll`, the file name is `llisapi`*<###>*`.out`.
  - For the Content Server servlet, the file name is `llservlet`*<###>*`.out`.

  The number <###> is generated by Content Server.

  Summary Timing logs
  If Summary Timing logs are enabled, Content Server generates logging on each called function, the SQL time taken, the output time taken, the mean execution time of each function, the user calling the function, and the originating IP address.

  Tip: Enabling Summary Timing logs on the **Configure Log Settings** page is equivalent to setting `Debug=11` in the `[general]` section of the `opentext.ini` file.

  Trace logs
  A Trace log file is generated whenever Content Server encounters an error condition that causes a script crash. It provides information on the module and script that caused the crash, and shows the variables and values that were being passed to or from the script at the time.

- The following logs can be enabled or disabled, but not configured:

  Socket Server logs
  Socket Server logs record communications sent from the Content Server service port (by default, 2099).

  Receiver logs
  Receiver logs record communications sent to the Content Server service port (by default, 2099).

Search Query logs

Enabling Search Query logs causes Content Server to log search transactions. Input, or queries, and output, or results, from the `otsearch` search engine, are logged to the `search.log` file in the *`<Content_Server_home>`*`/logs` folder.

Tip: Enabling Search Query logs on the **Configure Log Settings** page is equivalent to setting `wantSearchLogs=TRUE` in the `[options]` section of the `opentext.ini` file.

Note: Non-configurable log files are written to a subfolder of the *`<Content_Server_home>`*`\logs\` folder. For example, Socket Server logs are written to the *`<Content_Server_home>`*`/logs/socketServer_logs` folder.

- Links are provided to some other log types, including Rendition logging, Extractor logging and Archive Storage logging.

The following settings are available for the configurable log types:

Log Level

The log level can be set to one of the following levels:

0 - Off

Disables logging for Content Server, except for start-up logging. This is the default setting. If **No logging** is enabled, Content Server generates minimal startup log files, including one `thread`*`<#>`*`.out` file for each thread it starts.

1 - Warn

Provides minimal logging for Content Server.

2 - Info

Provides basic logging for Content Server.

3 - Debug

Provides verbose logging for Content Server.

4 - Trace

Provides all available logging for Content Server

Notes

- The available log levels vary by log type. For Summary Timing logs, only **0 - Off** and **2 - Info** are available. Trace Logs do not have log levels; they can only be enabled or disabled.
- The **3 - Debug** and **4 - Trace** log levels create very large log files and can have a negative effect on Content Server performance. In a production system, you should enable these levels only at the direction of OpenText Customer Support.

Location

The file location that the logs are written to. By default, logs are stored in the following subfolders of the *<Content_Server_home>*`\logs\` folder.

Thread Logs

`./logs/thread_logs/`

SQL Connect Logs

`./logs/connect_logs/`

Web Server Client Logs

`./logs/cgi_logs/`

Summary Timing Logs

`./logs/timing_logs/`

Trace Logs

`./logs/trace_logs/`

Rolling Logs

You can enable rolling log files, and specify the number of log files to retain before overwriting the oldest log file, and the size that a log file can reach before Content Server creates a new one. You can also enable compression of completed log files. By default, rolling log files are not enabled.

Note: This setting is not available for Trace log files.

Buffering

You can enable **Write immediately** or **Buffer in memory**. **Write immediately** guarantees that log output is written to a file. **Buffer in memory** permits faster performance but might, in some circumstances, mean that logging output is not written to a file. If you enable **Buffer in memory**, you can set the size of the buffer that must fill before Content Server writes the buffer’s contents to the log file. By default, **Write immediately** is enabled.

Note: This setting is not available for Trace Log files.

Retention

You can enable **Retention** to specify the maximum number of log files to retain and the number of files to delete if the total number of log files exceeds the **Number to keep**. By default, **Retention** is enabled, with **Number to keep** set to `1000` and **Number to delete when over limit** set to `50`.

Note: This setting is available only for Trace Log files.

The following options are available only in the Thread Logs section.

Note: The **Include request timing summaries** and **Include request parameters** settings apply to both Thread Logs and SQL Connect Logs. The **Include search and System Object logging** affects Thread Logs, but has no effect on SQL Connect Logs.

Options

Include request timing summaries

Timing summaries provide information on the duration of Content Server transactions. You can disable or enable the inclusion of request timing summaries in Thread logs. By default, request timing summaries are enabled.

Tip: Enabling **Include request timing summaries** is equivalent to setting `wantTimings=TRUE` in the `[options]` section of the `opentext.ini` file.

Include request parameters

Request parameters provide information on the parameters, including their current values, passed from the web browser to Content Server.

Tip: Enabling **Include request parameters** is equivalent to setting `wantVerbose=TRUE` in the `[options]` section of the `opentext.ini` file.

Include search and System Object logging

Enable this setting to include search and System Object logging information in the Thread log.

Tip: Enabling **Include search and System Object logging** is equivalent to setting `wantDebugSearch=TRUE` in the `[options]` section of the `opentext.ini` file.

User Logging

To generate level 3 (Debug) logging for requests from specific Content Server users, enter one or more Content Server user IDs in this box. If you enter more than one Content Server user ID, separate them with commas. This setting overrides the overall Log Level that is in effect for Thread logs, but only for the users entered in the **User Logging** box.

Tip: Enabling **User Logging** can be useful for troubleshooting specific problems. By using this setting, you can obtain detailed logging information on specific actions by specific users without having to enable verbose logging on all Content Server activity.

3.6 Configuring Presentation Settings

The **Configure Presentation** administrative pages enable you to set some of the basic appearance and behavior of Content Server. The settings on these pages affect browsing, sorting and filtering Content Server folders and other containers, the appearance of icons, and other such settings.

For information about configuring user password options and the user name display, see “Configuring User Settings” on page 427.

Configuring the Login Screen Message

Beginning with Content Server version 16.2.1, the login screen message is now configured in Directory Services. For information on configuring the login screen message, see the “Login Screen Message” system attribute in *OpenText Directory Services - Installation and Administration Guide (OTDS-IWC)*. For more information, see *OpenText Directory Services - Installation and Administration Guide (OTDS-IWC)* on OpenText My Support (https://knowledge.opentext.com/go/OTDS). Select **Documentation**.

3.6.1 Configuring Document Functions

On the **Configure Document Functions**, you can enable or disable the **Open** and **View as Web Page** functions for documents in Content Server. When these functions are enabled, users can open a document in its native application, or view it as a web page. When disabled, the **Open** option does not appear on a document’s **Functions** menu or on the **Overview** page. By default, **Open** is disabled and **View as Web Page** is enabled.

You can also enable or disable the **Overview** page as the default target for a link to a Document or a version of a Document. The **Document Overview** and **Version Overview** pages provide information about a Document or Version, and enable you to perform a number of functions on the Document or Version. For more information, see *OpenText Content Server - Documents and Text Documents (LLESWBD-UGD)*.

Tip: If the **Overview** page is not the default target for Document and Version links, you can still view it by selecting **Overview** from a Document's **Functions** menu.

To Configure Document Functions

To configure document functions:

1. In the **Server Configuration** section of the Content Server Administration page, click **Configure Presentation**.
2. On the **Configure Presentation** page, click **Configure Document Functions**.
3. On the **Configure Document Functions** page:

   a. Optional If you want the **Open** option to appear on all document's **Functions** menu, click **Enabled** next to **Open**.

   b. Optional If you want to activate the view as web page function for documents in Content Server, click **Enabled** next to **View as Web Page**.

   c. Optional If you want to ensure that document and version **Overview** pages are the default targets for any document or version link, next to **Overview** click **Enable**.
4. Click the **Save Changes** button to save your changes and return to the Administration page, or click **Cancel** to exit the page without making any changes.

3.6.2 Configuring Promoted Functions

You can make certain document-management functions easier to find in the user interface by *promoting* them. Promoted functions are displayed more prominently for Documents on the **Detail View** page of containers and Workspaces, and the **View as Web Page** and **Properties** pages for Documents.

The following functions can be promoted:

Function	Presentation
Download	A link on the Workspace or parent container's **Detail View** page and a button on the **View as Web Page** and **Properties** pages.
Edit	A link on the Workspace or parent container's **Detail View** page and a button on the **View as Web Page** and **Properties** pages.
Open	A link on the Workspace or parent container's **Detail View** page and a button on the **View as Web Page** and **Properties** pages.
Add Document	An **Add Document** button on the container's browse page.

Function	Presentation
Add Folder	An **Add Folder** button on the container's browse page.

Note: By default, both **Display on Detail List View** and **Display on Properties & View as Web Page** are enabled.

To Configure Promoted Functions

To configure promoted functions:

1. Click the **Configure Presentation** link in the **Server Configuration** section on the Administration page.
2. Click the **Configure Promoted Functions** link on the Configure Presentation page.
3. To display functions links for Documents on the Detail List View of a container, select the **Display on Detail List View** check box.
4. To display functions buttons on the Properties and View as Web Page pages of Documents, select the **Display on Properties & View as Web Page** check box.
5. Click the **Save Changes** button to save your changes and return to the previous screen, or the **Cancel** button to cancel your changes and return to the main Administration page.

3.6.3 Configuring the Sidebar

You can enable or disable the **Content Filter** sidebar and sidebar panels for all users. By default, both are enabled.

To Configure the Sidebar

To configure the sidebar:

1. On the Content Server Administration page, click **Server Configuration**.
2. Select **Configure Presentation**, then **Configure Sidebar**.
3. To enable the sidebar for all users, ensure the **Enable Sidebar** check box is checked. The sidebar is enabled for all users by default.
4. In order to ensure that the sidebar is enabled for all users, you must also select at least one sidebar panel. By default, the Content Filter sidebar panel check box is checked.
5. Click the **Save Changes** button to save your changes and return to the previous page, or click the **Reset** button to cancel your changes.

Notes

- If there is only one sidebar panel available to enable, disabling that panel will disable the sidebar. In order to ensure that the sidebar is enabled for users, you must select the **Enable Sidebar** check box and one sidebar panel.
- You can also configure the sidebar from the Facets Volume Control Panel page. Click the **Enterprise** global menu, and then click **Facets Volume**. From the **Facets** functions menu, select **Control Panel**. Select **Configure Sidebar**.

3.6.4 Configuring Small and Large Icon Views

You can enable or disable small and large icon views in the user interface. When the **Display Large and Small Icon Views** setting is enabled, containers can display items using the Detail, Large, and Small Icon Views and users can toggle between view types using the **View Type** buttons. By default, items marked as Featured will appear in both the **Featured Items** section and in the **Detail View** list. The administrator can change this default in the **Featured Items** section.

When this setting is disabled, users cannot toggle between views. The **Detail View** displays for all containers, regardless of which view the user had previously selected in for the container. If you re-enable the **Display Large and Small Icon Views** setting, the container will display the view that was originally selected.

Note: The **Display Large and Small Icon Views** setting is disabled by default.

To Enable or Disable Small or Large Icon Views

To enable or disable small or large icon views:

1. Click the **Configure Presentation** link in the **Server Configuration** section on the Administration page.
2. On the Configure Presentation page, click the **Configure Small and Large Icon Views** link.
3. On the Configure Small and Large Icon Views page, select or clear the **Display Small and Large Icon Views** check box, and then click the **Save Changes** button.

3.6.5 Configuring Project Presentation Settings

This page allows you to configure the following default Project appearance and behavior:

- You can set the default start page for a Project to either the Project's **Overview** page or the Project Workspace.
- You can display either a **Project** menu or a **Project Icon Bar** in all Project Workspaces.
- You can enable the `Overview.html` page, which provides Project participants with a personalized view of items in a Project. The sections that appear on the page are configured by the Project Coordinator. When this option is enabled, the `Overview.html` page appears when a Project is opened. By default, this option is disabled, and the **Project Workspace** page is used as the start page when a Project is opened.
- You can set the maximum number of items allowable in each section on the **Project Overview** page.
- You can change the default Status Indicator values for all Projects.

Note: When you change a Project setting, the change applies to new Projects *and* existing Projects. For example, if you clear the **My Tasks** check box in the **Navigation** section, the **My Tasks** icon will no longer display in the Project Icon Bar.

To Configure Project Settings

To configure Project settings:

1. Click the **Configure Presentation** link in the **Server Configuration** section on the Administration page.
2. Click the **Project Settings** link on the Configure Presentation page.
3. In the **Start Page** section, click either the **Overview** or **Workspace** radio button.

   This determines the first page that appears when a user opens a Project.
4. In the **Overview.html** section, click the **Enable** or **Disable** radio button.
5. In the **Navigation** section, select the **Project Menu** check box to display the **Project** menu in all Project Workspaces.
6. Do one of the following:
   - Select the **Project Icon Bar** check box, and then select the check boxes of the items you want displayed in the Icon Bar.
   - Clear the **Project Icon Bar** check box if you do not want the Icon Bar.

7. In the **Overview Settings** section, select the check boxes of the sections you want to allow Project Coordinators to choose from when selecting sections to appear on the Project Overview page.

8. In the # **of items** drop-down list, click the maximum number of items allowable in each section on the Project Overview page.

9. In the **Status Indicator** section, type a value for each of the status indicators in the appropriate fields.

   Note: If you change the default Status Indicator values and there are existing Projects, the existing Projects pick up the new values immediately. You should advise Project Coordinators of any impending changes prior to submitting the change.

10. Click the **Submit** button.

3.7 Configuring Smart View Default Style and Online Help

The Configure Smart View page allows you to change default settings for the Content Server Smart View user interface.

Enable users to open Classic View

When users access the Content Server Smart View, the **Classic View** option on the **My Profile** menu appears by default. To hide this menu option, clear the **Enable Classic View menu item** check box on the Configure Smart View administration page.

Enable Apple mobile device support when sharing objects from Smart View

When users share content in the Content Server Smart View, Content Server generates an email that contains a URL to the Content Server object. When a recipient tries to open the link on an Apple® device, the default URL does not work. Select the **Enable Apple mobile device support** check box to generate a second URL that is supported on Apple devices.

Overriding Default Style

The Overriding Default Style setting allows you override the default style that appears in Content Server Smart View. The override is done by deploying an additional stylesheet to the `/support` directory, then adding the relative or absolute path to the file in the **URL Path** parameter. The styles specified in the new stylesheet will override the styles in the default stylesheet.

An additional dark theme is available for Content Server that includes a transparent header, darker background gradient, and darker breadcrumbs. To apply the dark theme, you modify the `overrides.css` style sheet. The default location for the style sheet is: `/img/csui/themes/dark/overrides.css`, where `/img` is the URL Prefix for the `/support` directory.

Alternate Online Help Server

The online help for the Smart View user interface uses the OpenText™ Help System, which includes the OpenText Global Help Server. The Global Help Server is a live help system that requires internet access to view the latest online help.

The settings on this page are used to configure an OpenText Private Help Server, which is an alternative method of viewing the online help. This method is available for users who do not have access to the internet.

Private Help Server settings:

Important
Changing these values can cause the online help to become inaccessible. Do not change these values unless instructed to do so by OpenText Customer Support.

- **URL Root** – The root URL for an OpenText Private Help Server you install and configure. For more information about setting up a Private Help Server, see *OpenText Content Server - Installation Guide (LLESCOR-IGD)*.
- **Type** – A custom help type. The default value is `ofh1`.
- **Tenant** – A custom help tenant value.

Supported subtypes for Recently Accessed tile

The Recently Accessed tile lists items that users have recently opened. This setting allows you to customize the Recently Accessed tile by selecting which items are included on the tile, or by removing items that are included by default.

User Profile Settings

You can do the following to configure user profiles in Smart View:

- Enable the simple user profile format. Simple user profiles only display the user’s name, email, office location, phone number, and manager’s name. If Pulse is disabled, the manager’s name is not displayed.
- Enable profile pictures. This setting enables users to upload and display profile pictures in Smart View.

  Note: If you disable this setting, user name initials will be displayed instead of profile pictures. Users will still be able to upload profile pictures in Classic View, but these pictures will not be displayed in Smart View.

3.7.1 To Enable or Disable the Classic View Menu Option

To enable or disable the Classic View menu option:

1. Click the **Configure Smart View** link in the **Server Configuration** section of the Administration page.
2. In the **Enable users to open Classic View** section on the Configure Smart View page, select the **Enable Classic View menu item** check box to allow users to access the Classic View user interface from Smart View, or clear the check box to disable the option. When enabled, the **Classic View** option appears on the **My Profile** menu in Content Server Smart View.
3. Click **Save Changes**.

3.7.2 To Enable or Disable Apple Mobile Device Support

To enable or disable Apple mobile device support:

1. Click the **Configure Smart View** link in the **Server Configuration** section of the Administration page.
2. In the **Enable Apple mobile device support when sharing objects from the Smart View** section on the Configure Smart View page, select the **Enable Apple mobile device support** check box to generate a URL that is supported on Apple devices, or clear the check box to turn off this feature.
3. Click **Save Changes**.

3.7.3 To Configure a Private Help Server

To configure a Private Help Server:

> **Important**
> Changing these values can cause the online help to become inaccessible. Do not change these values unless instructed to do so by OpenText Customer Support.

1. Click the **Configure Smart View** link in the **Server Configuration** section of the Administration page.
2. In the **Alternate Online Help Server** section of the Configure Smart View page, specify any of the Private Help Server settings, and then click **Save Changes**.

3.7.4 To Change the Smart View Default Style

To change the Smart View default style:

1. Click the **Configure Smart View** link in the **Server Configuration** section of the Administration page.
2. In the **Overriding Default Style** section on the Configure Smart View page, type the absolute URL path to the CSS stylesheet you want applied to the Smart View, and then click **Save Changes**.

3.7.5 To Configure Subtypes for the Recently Accessed Tile

To configure subtypes for the Recently Accessed tile:

1. Click the **Configure Smart View** link in the **Server Configuration** section of the Administration page.
2. In the **Supported subtypes for Recently Accessed tile** section on the Configure Smart View page, click the **Edit** icon.
3. On the Configure Recently Accessed tile page, select the check box for each item type that you want included on the Recently Accessed tile, and then click **Save**.
4. Click **Save Changes**.

3.7.6 To Configure User Profile Settings

To configure user profile settings:

1. Click the **Configure Smart View** link in the **Server Configuration** section of the Administration page.
2. In the **User Profile in Smart View** section, do one or both of the following:
   - Select the **Enable Simple User Profile** check box to enable simple user profiles in Smart View.
   - Select the **Enable Profile Picture** check box to enable users to upload and display profile pictures in Smart View.
3. Click **Save Changes**.

3.8 Configuring System Messages

The System Messages feature enables the administrator to broadcast information to all users on the system using the News Player. News players deliver information to the Enterprise Workspace, all Personal Workspaces, and some other Content Server pages.

3.8.1 To Configure System Messages

To configure system messages:

1. Click the **Configure System Messages** link in the **Server Configuration** section on the Administration page.
2. To add a system message, do the following:
   - Click the **Add Message** button.
   - Type a name for the message in the **Name** field.
   - Type a headline describing the message in the **Headline** field. This is the text that will appear in the News Player.
   - Optionally, type a URL in the **URL** field. Specifying a URL makes the headline a clickable link that will take the user to another webpage. This can be any webpage that can be accessed by Content Server, either on the Internet, on your organization's intranet, or within Content Server itself.
   - Click the date on which you want the message to begin appearing to users in the **Effective Date** drop-down lists.
   - Click the ⇧ and ⇩ buttons to move the item either up or down in the menu order.
   - Click the **Submit** button to save your changes and return to the Content Server Administration page. Click the **Cancel** button to cancel your changes and return the page to its previous saved values so you can begin again.
3. To edit a system message, do the following:
   - Click to highlight the name of the message you want to edit in the dialogue box on the left hand side of the **Configure System Messages** page.
   - You will note that the fields on the right hand side of the page are now populated with the message information associated with the message name you highlighted. Edit the information in the appropriate fields.
   - Click the ⇧ and ⇩ buttons to move the selected item either up or down in the display order.

Tip: To delete a message, click to highlight the name of the message you want to delete in the dialogue box on the left hand side of the **Configure System Messages** page. Click the **Delete** ☒button.

3.9 Customizing the User Interface with Appearances

An *Appearance* is a container that stores Documents and HTML code. Appearances enable you to customize certain locations, much as you would design a webpage. For information about Appearances, see *OpenText Content Server - Custom Views and Appearances (LLESAPP-UGD)*.

Global Appearances, which are intended to be applied to multiple, separate locations, must be added to the Appearances Volume. To add Global Appearances, you need the Add Items permission on the Appearances Volume.

The Appearances Volume is accessible from the Administration page.

1. Select **Appearances Administration**.
2. Next, select **Open the Appearances Volume**.
3. To create a Global Appearance, click the **Add Item** button and select **Global Appearance**.
4. Type a name for the new global appearance in the **Name** field. Optionally, type or select items in the **Description**, **Categories**, and **Create In** fields.
5. Click the **Add** button.

Chapter 4

Configuring and Customizing Faceted Browsing

If you are a Knowledge Manager or an administrator, you can access the Facets Volume from the **Enterprise** menu on the global menu bar. (If you are an administrator, you can also access the Facets Volume from the Content Server Administration page.) If the link to access the Facets Volume is not available to you, you do not have the necessary privileges. Contact your administrator for access to the Facets Volume.

4.1 Configuring Faceted Browsing

Faceted Browsing is one of the navigational tools available to Content Server users. It allows you to filter your view of items in Content Server using groupings of metadata, or facets, to make it easy to locate items of interest. Faceted Browsing is enabled by default and is installed with default facets and document classes. As an administrator, you need to assess the needs of your users to determine how you will customize faceted browsing. This section describes how to configure faceted browsing for all users so that the facets available are relevant to your system's content. It details how to configure the sidebar for all users, set up Knowledge Managers, and add document classes, facets, facet trees, and columns.

Tip: For information on using faceted browsing, see *OpenText Content Server - Documents and Text Documents (LLESWBD-UGD)*.

Enabling Faceted Browsing

Faceted browsing is enabled by default for all users. It is accessed by users through the **Content Filter** sidebar. As an administrator, you can disable the sidebar for all users.

For information about enabling and configuring the **Content Filter** sidebar, see “To Configure the Sidebar” on page 40.

Configuring Knowledge Managers

The administrator must decide who, in your organization, has sufficient knowledge of your organization's content to serve as a Knowledge Manager. Only an administrator can define a Knowledge Manager. The system administrator gives the person designated as a Knowledge Manager the privileges and permissions necessary to access the Facets Volume so that they can administer the faceted browsing setup. Knowledge Managers structure faceted browsing for your organization.

Tip: OpenText recommends that you create a Knowledge Manager group in Content Server and then populate that group with the users who will be assigned the Knowledge Manager privilege.

Configuring Document Classes

A Document class is a facet data source that groups classes of documents to make it easier and more intuitive to find certain kinds of documents. For example, the Media document class allows you to filter your view of Content Server so that you only see Audio and Video documents.

Document Classes are composed of MIMEType Aliases, which are groupings of MIME types. For example, the Audio MIMEType Alias is composed of numerous MIME types that identify audio files, including `audio/wav`, `audio/mpeg3`, and `audio/x-mpeg-3`. The Audio MIMEType AliasContent Server allows you to search for audio files by MIME type, without actually needing to know and specify the numerous MIME types that an audio file could have.

To suit your organization’s needs, you can modify the default Content Server document classes and their underlying MIMEType Aliases. You can also add and configure new ones. When you configure a MIMEType Alias, you select the MIME types that make up the document class on the **Configure MIMEType alias** page. MIME types are categorized as follows:

- **MIMETypes in use**

  The MIME types of items that exist in your Content Server system. Any document, graphic file, or other item that has been added to a location in Content Server has a MIME type. That MIME type is listed in this section.

- **MIMEType Aliases**

  MIMEType aliases that have already been defined within all document classes.

- **Known MIMETypes**

  MIME types in this section are known to exist, but do not apply to any item currently in your Content Server system, and so do not appear in the **MIMETypes in use** section.

No document class can be deleted if it is being used as a data source for a facet. If you attempt to remove a document class that is a data source for a facet, Content Server informs you that the document class cannot be deleted.

Configuring the Date Format

Date facets can be sorted using a variety of modifiers. Relative, Year, and Month modifiers have a single default appearance that cannot be modified, but the appearance of the Day modifier depends on the Content Server **Short Date Display Format**. You can change the appearance of days in a Date facet by changing the **Short Date Display Format** on the **Administer Date/Time** administration page. For more information, see “Setting Date and Time Formats” on page 30.

Important
Changing the short date display format affects the appearance of dates throughout Content Server. It does not affect only the appearance of the Day modifier for date facets.

4.1.1 To Set Up Knowledge Managers

To set up Knowledge Managers:

1. On the Content Server Administration page, in the **System Administration** section, click **Administer Usage Privileges**.
2. On the **Administer Usage Privileges** page, under the column **Usage Type**, find **Facet Administration**. The **Usage Name** is Knowledge Manager and its **Usage Status** is restricted, by default. Click **Edit Restrictions**.
3. On the **Edit Group: Knowledge Manager** page, add the user or group that you want to designate as a Knowledge Manager, and then click **Done**
4. After adding the user or group to the Knowledge Manager group, give it permission to edit the Facets Volume.

   a. Click **Facets Volume** on the **Enterprise** global menu.
   b. On the **Facets** Functions menu, click **Permissions**.
   c. Click **Grant Access** in the **Assigned Access** section.
   d. Enter the name of your new Knowledge Manager user or group in the filter box, and then click **Find**. Enable **Grant Access** beside the name of the user or group, and then click **Submit**.
   e. Enable the permissions that you want to assign to your Knowledge Manager. OpenText recommends that you grant the **Edit Permissions** access level.
   f. Click **Update**, and then click **Done**.

4.1.2 To Add and Configure a Document Class

To add a document class:

1. Open the **Document Class Definitions** page by one of the following methods

   - On the Content Server Administration page, under **Server Configuration**, click **Configure Facets**. On the **Configure Facets** page, click **Configure Document Classes**.
   - Click **Facets Volume** on the **Enterprise** global menu. On the **Facets** Functions menu, click **Control Panel**. On the **Facets Volume Control Panel** page, click **Configure Document Classes**.

2. In the **Document Classes** box, type the name of the new document class, and then click **Add New Document Class**.

Tip: To remove a document class, click **Delete** <*Document_Class*> (⊟) under **Actions**.

3. To configure your new document class, click the new document class name under **Class Name**. You now see the **MIMEType Alias Definitions** page.

   Note: You can add or delete a MIMEType Alias for any existing document class. To add or delete a MIMEType Alias for an existing document class, click the document class under **Class Name**.

4. On the **MIMEType Alias Definitions** page, enter an Alias Name for your new document class. Click **Add New Alias** to the right of the **MIMEType Aliases** box to add the new Alias to the **Alias Name** list.

   Note: To remove a MIMEType Alias, click **Delete** <*Alias_Name*> (⊟), under **Actions**.

5. To configure your new Alias, click the new Alias Name. The **Configure MIMEType alias** page appears. In the **Configure MIMEType alias** page, enable all of the MIME types that you want to add to your new MIMEType Alias. Once you have finished, scroll to the bottom of the screen and click **Update**.

4.2 Working with the Facets Volume

The Facets Volume is available to Content Server administrators and Knowledge Managers. If the link to access the Facets Volume is not available to you, you do not have the necessary privileges. Contact your administrator for access to the Facets Volume.

In the Facets Volume, you can add *columns*, *facets*, *facet folders* and *facet trees*. OpenText recommends that, before you create a column, facet, or facet tree, you first create a facet folder to store your custom items. This will aid in future maintenance of your faceted browsing deployment.

4.2.1 Columns

In the Browse View of any location, items are viewed in a list. For each item in the list, Content Server displays values in the columns that are defined for the Browse View. If a column is sortable, clicking its name re-orders the list.

Content Server has two kinds of columns: Fixed System Columns and custom columns. Fixed System Columns are installed by default and cannot be removed from Content Server. Custom columns are added to your Content Server deployment by a Knowledge Manager or a Content Server administrator. Two of the Fixed System Columns must always appear in the Content Server interface: **Type** and **Name**. The other Fixed System Columns can be added to the Content Server interface or removed from it, according to your organization’s needs. See “Configuring Global Columns” on page 68.

Knowledge Managers and Content Server administrators can create new custom columns for users to view and use. To add a column, click **Add Item**, select Column and, on the **Add: Column** page, select a data source for your column.

Data sources are made available by a Content Server administrator. They are based on Content Server metadata, including Category Attributes and Classifications. When you create a column, you choose a data source from a list that contains active unused data sources. If a data source has been used, it does not appear in the list. You cannot use the same data source twice.

After you have created a custom column, you should configure its appearance and behavior, and set its availability and permissions.

Configuring a Custom Column

To configure a custom column, click **Properties** > **Specific** on the column's **Functions** menu. The **Specific** Properties page provides the following information:

- **Column data source**

  The data source that was selected when the column was created.

- **Status**

  The current status of the column. There is also a **Rebuild Column** button that you can use, if necessary.

- **Sortable**

  Indicates whether the column can be sorted by users.

- **Width**

  The width of the custom column in characters. The default setting is 20. Allowable values range from 1 to 250. This field is required.

  Note: A custom column displays a maximum of 64 characters of data. If the length of the data to be displayed in the column exceeds 64 characters, the text is truncated and suspension points (...) appear to represent the missing data. Setting the column width to a value greater than 64 characters does not affect this limitation.

- **Alignment**

  Determines whether the column text aligns **Left**, **Center** or **Right**. The default alignment is **Center**.

- **Long Text**

  Determines how column text that is wider than the column appears: **Wrap**, **Don’t Wrap**, or **Truncate**. The default setting is **Wrap**.

- **Display as link?**

  If selected, this setting makes the column value appear as a hypertext link.

This setting is enabled by default if the column data source is a user-type data source. If it is not enabled, the next four options cannot be configured. If **Display as link?** is enabled, the **Link URL** and **Display value** fields below are required.

- **Link URL**

  The URL that the column value links to. You can use any of the **Display value** variables in the URL. For example, to add a column based on the **Advanced Version** data source and have it display a link that opens the **Version** properties page for an item, accept the URL that is provided by default for the **Link URL**: `?func=ll&objId=%objid%&objAction=versionproperties&vernum=%versionnum%&nexturl=%nexturl%`

- **Display value**

  The value to be displayed in the column. The default value is `%value%`, which displays the value for the column. Other options are:

  - **%nexturl%**

    The URL the browser will be directed to after the original action has been completed.

  - **%objid%**

    The ID of the Content Server item.

  - **%rawvalue%**

    The raw value for the Content Server item.

  - **%value%**

    The value for the column. This is the default value.

  - **%versionnum%**

    The number of the latest item version that the user has permission to see.

- **Alt-text**

  The alt-text for the link. You can use any of the **Display Value** variables in this setting.

- **Link Target**

  If this setting is selected, the **Link URL** opens in a new browser window.

Column Availability

To allow users to access a custom column, make it available on its **Availability** Properties page. (You do not need to set the availability of a Fixed System Column. Fixed System Columns are always available.) The availability options for your custom column are **Not available**, **Available everywhere** or **Only available in specific locations**. By default, a custom column is **Not available**.

Note: For a custom column to appear in the Content Server interface, in addition to being made available, it must be configured to appear in a Folder’s **Column** properties in one of the following manners:

- in the global columns,
- at the folder level
- in a user's personal settings.

Column Permissions

Users require permission to see, edit, or administer the column. The permissions that you can assign are **Administer**, **Read**, **Write** and **None**. By default, a custom column is given a Public Access permission of **Read**. OpenText recommends that you keep this setting.

For information about setting permissions for your column, see “Administering Permissions“ on page 11.

4.2.2 Facets

The facet panel appears in the **Content Filter** sidebar. It displays facets and facet values derived from metadata belonging to the items in the current container and its sub-containers. Metadata are values that describe an item. Facets are groupings of items that have the same or similar metadata values.

System Default Facets (**Owner**, **Content Type**, **Document Type**, and **Modified Date**) appear in the Browse View by default. Knowledge Managers can create and edit custom facets in the **Facets Volume**.

A user sees a facet in Content Server if all of the following is true:

- The facet's status is `Ready`.
- The **Display in sidebar** setting is enabled.
- The user has permission to access the facet.
- The user has permission to access the category that is the basis of the data source (if the facet uses a category as its data source).
- The facet is in a facet tree.
- The user has permission to access the facet tree.
- The facet tree is available for the user’s current location.

The first step in creating a facet is choosing a data source. Your administrator is responsible for managing your available data sources. Only active and unused data sources appear in the list of data sources for a facet. Once a data source is in use, it no longer appears in the list.

Any category that resides in the Categories Volume can serve as a data source. Categories and attributes appear in the **Data Source** list as: **Category:** **<***Category_Name***>:<***Attribute_Name***>**. An attribute in a **Set** attribute appears as: **Category:** **<***Category_Name***>:<***Set_Name***>:<***Attribute_Name***>**. The data source field list is alphabetically listed, followed by a separator, and then all available attributes.

To configure a custom (non-default) facet, click **Properties** > **Specific** on the facet's Functions menu. The fields on the **Specific** tab of a facet's Properties page are:

- **Facet data source**

  Displays the facet's data source.

- **Status**

  Displays the current status of the facet and provides a button to rebuild the facet. The facet's status can be **Building**, **Ready**, or **Error**.

- **Show in sidebar**

  Determines whether the facet appears in the **Content Filter** sidebar. This setting is enabled by default. Disabling it removes the facet from the sidebar, but keeps it in the facet tree definition.

- **Minimum unique values**

  The minimum number of unique values required before the facet may appear. The default setting is 2.

- **Maximum values to display**

  The maximum number of unique values permitted to appear in the facet. The maximum value is 20. The default setting is 5.

- **Display mode**

  Specifies the order in which facet values are displayed. The default setting is **Ranked list**.

  The available options depend on the type of facet. Generally, the options available are:

  - **Ranked list**: orders by the count for each value, with the most common values appearing first.
  - **Alphabetical list**: orders by the name of the value.

  Date facets do not support display mode.

- **Display priority**

  A box that specifies how prominently the facet is displayed in the **Content Filter** sidebar. Facets with a display priority of **High** appear above facets with a display priority of **Medium** or **Low**. Facets with a display priority of **Low** appear below facets with a display priority of **Medium** or **High**. The default setting is **Medium**.

- **Display count**

  Determines whether or not the facet item count is displayed in the **Content Filter** sidebar. You can select **Approximate** or **Do not display**. The default setting is **Approximate**, which means that the facet item count is displayed to three significant digits for regular Content Server and the actual facet item count is displayed to Content Server Administrators. Administrators should bear in mind however that, because of the dynamic nature of the Facets subsystem, the actual facet item count is still an approximate value.

- **Show lookup in 'More...'**

  Adds a filter box to the **More** dialog box, if the facet type is filterable. (Text and user facet types are filterable.) You can use the lookup box to filter items by facet value. This setting is enabled by default.

A facet can be assigned a permission of **Administer**, **Read**, **Write**, or **None**. By default, a custom facet is given a Public Access permission of **Read**. OpenText recommends that you keep this setting. The Public Access permission value is cached with the facet and facet tree definitions. This results in significantly faster browse time because Content Server does not have to check user permissions on the facets and facet trees. For information about setting permissions for your facet, see “Administering Permissions“ on page 11.

After you create a facet, include it in a facet tree to make it available. (Your facet is not available unless it is included in a facet tree.) For information about including your facet in a facet tree, see “To Configure a Facet Tree” on page 63.

Tip: A facet that is used in the definition of a facet tree cannot be deleted. The facet must first be removed from the definition of a facet tree before it can be deleted.

4.2.3 Facet Folders

Facet Folders provide a way to manage and organize your custom environment. Columns, facets, and facet trees can have their permissions set so that they are only accessible by certain groups in Content Server. When creating custom items in the Facets Volume, you should consider first creating a facet folder to store the new custom item. For example, if you are creating custom Facets Volume items for your Financial Department, you could create a facet folder called `Financial Dept`. This will help with future maintenance for your custom items.

4.2.4 Facet Tree

A Facet Tree is used to list the facets that appear in the **Content Filter** sidebar. Facet Trees allow the Knowledge Manager to determine which users see facets and which locations they appear in.

To give users access to a facet tree, make the facet tree available on the **Availability** tab of your facet tree's **Properties** page, and give your users permission to see it.

The availability options for a facet tree are:

- **Never displayed**

  The facet tree is never displayed in the **Content Filter** sidebar. This is the default option.

- **Display in all facet sidebars**

  The facet tree always appears in the **Content Filter** sidebar, if the user has sufficient permissions to see it.

- **Only available in specific locations**

  The facet tree appears in the **Content Filter** sidebar panel only in the locations selected in the **Locations** box. (The **Locations** box allows you to select the Enterprise Workspace, a Folder, or a Project.) Users must also have sufficient permissions to see the facet tree.

Allowable permissions are **Administer**, **Read**, **Write**, and **None**. By default, a custom facet tree is given a Public Access permission of **Read**. OpenText recommends that you keep this setting. For information about setting permissions for your facet tree, see “Administering Permissions“ on page 11.

You can also control whether a Facet Tree appears in a given location by editing the following sections of that container’s **Presentation** properties page:

- **Global Trees**

  Displays a list of the facet trees that are available globally. The trees are displayed in alphabetical order by facet tree name. Each tree is displayed as a link that takes you to the **Availability** tab for the related facet tree in the Facets Volume.

  If there are no trees to display for this field, `No global facet trees found` is displayed.

- **Inherited Trees**

  Displays a list of the facet trees that are available at the current folder or inherited from a parent object. The facet trees are displayed in alphabetical order by name. Each tree appears as a link that takes you to the **Availability** tab of the facet tree in the Facets Volume. The name of the location from which the tree is inherited appears in light-gray text to the right of the facet tree link. The name of the location is not displayed if the user does not have permission to view the object.

  If there are no trees to display for this field, `No inherited facet trees found` is displayed.

- **Local Trees**

  Contains an editable list of facet trees that are specifically made available to the current folder, displayed in alphabetical order.

  Clicking **Select** allows a Knowledge Manager to select facet trees from the Facets Volume to add to the list of Local Trees. Facet trees that already appear in the list of Local Trees for the current folder are not added if they are selected again.

  The **Remove** button is disabled until at least one facet tree is selected in the list of Local Trees. Clicking **Remove** deletes the selected facet trees from the list of Local Trees.

4.2.5 Viewing the Facets Volume

The **Facets Volume** is available only to administrators and Knowledge Managers. If you are not able to view the **Facets Volume**, contact your administrator to request the appropriate permissions.

Use one of the following methods to open the **Facets Volume Control Panel**.

- On the **Enterprise** menu, click **Facets Volume**.
- If you are a Content Server administrator, in the **Server Configuration** section of the Content Server Administration page, click **Server Configuration**, click **Configure Facets**. Then, on the **Configure Facets**page, click **View Facet Volume**.

4.2.6 To Add a Column

To add a Column:

1. On the **Enterprise** menu, click **Facets Volume**.
2. Optional Browse to the custom facet folder in which you want to create your new column, or create a facet folder in the Facets Volume then browse to that new folder.
3. On the **Add Item** menu, click **Column**.
4. In the **Name** field, type a unique name for your new column.
5. Optional In the **Description** field, type a description for your new column.
6. In the **Data Source** box, choose a data source for your new column.
7. Optional In the **Categories** field, click **Edit** to apply a Category to this column.
8. Optional If you want to store the column in a location other than that which appears in the **Create In** field, click **Browse Content Server**, browse to the container where you want to locate the column, and then click **Select**. Only those areas in Content Server that can store a column will be selectable.
9. Click **Add** to save your new column and return to the Facets Volume.

4.2.7 To Configure a Column

To configure a Column:

1. Once you have created your custom column, you will find yourself back in the facet folder in which you created your custom column.

   From your new column's Functions menu, click **Properties**, and then click **Specific**.
2. On the **Column Properties: <*Column_Name*>** page, in the **Width** field, set the desired width of the column in characters.

Note: A custom column displays a maximum of 64 characters of data. If the length of the data to be displayed in the column exceeds 64 characters, the text is truncated and suspension points (...) appear to represent the missing data. Setting the column width to a value greater than 64 characters does not affect this limitation.

3. In the **Alignment** field, select the alignment for your column from the list.
4. In the **Long Text** field, select whether the column text will wrap or not from the list.
5. Enable **Display as link?** to allow the column value to display as a hypertext link.
6. In the **Link URL** text box, enter the URL to which the column value will link.
7. In the **Display value** field, enter the value that will display in the column.
8. In the **Alt-text** input box, enter the alt-text for the link.
9. Enable **Link Target** to make the link open in a new browser window.
10. Click **Update** to save your new column settings and return to the facet folder.

To make a Column available to users:

1. To set your new column's availability and permissions settings, on the Functions menu for your column, click **Properties** and then click **Availability**.
2. In the field **Column availability**, select one of **Not available**, **Available everywhere** or **Only available in specific locations**.
3. If you selected one of **Not available** or **Available everywhere**, click **Update** to save your changes and return to the facet folder.

   If you selected **Only available in specific locations**, click **Browse Content Server** next to the **Locations** box to select those locations in Content Server that will display your custom column. Once you have selected your locations, click **Update** to save your changes and return to the facet folder.
4. On the Functions menu for your column, click **Properties**, and then click **Permissions**.
5. On the **Permissions** page for your column, select the user or user group whose permission you want to edit. In the **Edit User Permissions** dialog box, enable the permission that you want to assign.
6. Click **Update** to save your changes.
7. Click **Done** to return to the facet folder.

4.2.8 To Add a Facet

To add a Facet:

1. On the **Enterprise** global menu, click **Facets Volume**.
2. Optional Browse to the custom facet folder in which you want to create your new facet, or create a facet folder in the Facets Volume and then browse to that new folder.
3. On the **Add Item** menu, click **Facet**.
4. In the **Name** box, type a unique name for your new facet.
5. Optional In the **Description** field, type a description for your new facet.
6. In the **Data Source** box, select a data source for your new facet.
7. Optional In the **Categories** field, click **Edit** to apply a Category to this facet.
8. Optional If you want to place the facet in a location other than that which appears in the **Create In** field, click **Browse Content Server**, browse to the container where you want to locate the facet, and then click **Select**. Only those areas in Content Server that can store a facet will be selectable.
9. Click **Add** to save your new facet and return to the Facets Volume.

4.2.9 To Configure a Facet

After you create a custom facet, you are returned to the facet folder in which you created your facet.

To Configure a Facet:

1. On the facet's Functions menu, click **Properties**, and then click **Specific**.
2. On the **Facet Properties: <***Facet_Name***>** page, enable **Show in sidebar** to ensure that the facet appears in the **Content Filter** sidebar.
3. In the **Minimum unique values** box, select the minimum number of unique values required to cause the facet to appear in the sidebar.
4. In the **Maximum values to display** list, select the maximum number of unique values that can appear in the facet before a **More** link appears.
5. In the **Display mode** list, select the order in which facet values are displayed.

   Note: The available options depend on the type of the Facet. Date facets do not support display mode.

6. In the **Display priority** list, select a value to determine whether the facet appears near the top of the sidebar (**High**), towards the bottom (**Low**), or in the middle (**Medium**).

7. In the **Count accuracy** list, select the level of accuracy for the facet item count.
8. Enable **Show lookup in** '**More...**' to add a filter box to the **More** dialog box if the facet is a type (Text or User) that supports filtering.
9. Click **Update** to save your new facet settings and return to the facet folder.

To make a Facet available to users:

1. On the Functions menu for your new facet, click **Properties** and then click **Permissions**.
2. On the **Permissions** page for your facet, select the user or user group whose permissions you want to edit. On the **Edit User Permissions** page, enable the permissions that you want to assign.
3. Click **Update** to save your changes.
4. Click **Done** to return to the facet folder.

4.2.10 To Add a Facet Folder

To add a Facet Folder:

1. On the **Enterprise** global menu, click **Facets Volume**.
2. On the **Add Item** menu, click **Facet Folder**.

   Tip: Your administrator can enable an **Add Facet Folder** button to the left of the **Add Item** menu.

3. In the **Name** field, type a unique name for your new facet folder.
4. Optional In the **Description** field, type a description for your facet folder.
5. Optional In the **Categories** field, click **Edit** to apply a Category to this facet folder.
6. Optional If you want to place the facet folder in a location other than that which appears in the **Create In** field, click **Browse Content Server**, browse to the container where you want to locate the facet folder, and then click **Select**. Only those areas in Content Server that can store a facet folder will be selectable.
7. Click **Add** to save your new facet folder and return to the Facets Volume.

4.2.11 To Add a Facet Tree

To add a Facet Tree:

1. On the **Enterprise** global menu, click **Facets Volume**.
2. Optional Browse to the custom facet folder in which you want to create your new facet tree, or create a facet folder in the Facets Volume and then browse to that new folder.
3. Click **Add Item**, and then click **Facet Tree**.
4. In the **Name** field, type a unique name for your new facet tree.
5. Optional In the **Description** field, type a description for your new facet tree.
6. Optional In the **Categories** field, click **Edit** to apply a Category to this facet tree.
7. Optional If you want to place the facet tree in a location other than that which appears in the **Create In** field, click **Browse Content Server**, browse to the container where you want to locate the facet tree, and then click **Select**. Only those areas in Content Server that can store a facet will be selectable.
8. Click **Add** to create your new facet tree and return to the Facets Volume.

4.2.12 To Configure a Facet Tree

To Configure a Facet Tree:

1. On the facet tree's Functions menu, click **Properties**, and then click **Specific**.
2. On the **Facet Tree Properties: <***Facet_Tree_Name***>** page, in the **Facet Tree definition** box, you see the name of the facet tree. To the right of the facet tree name, you see an **Add Child Facet** icon (➕). To begin creating the tree, click **Add Child Facet**.
3. A new level to your tree appears, along with a box that allows you to select a facet to add to your tree. Select the facet that will become your new level 1 for your facet tree.
4. To the right of the level 1 facet you have just added to your facet tree, you see **Add** (➕)and **Remove** (➖) buttons. To add a second level to your facet tree, click **Add Child Facet**. If you wish to remove the level 1 facet you have just added, click **Remove**.

   Note: Creating a child facet from your facet tree name creates a level 1 facet in your tree. Creating child facets on each subsequent level will add a new level to your tree.

5. Click **Update** to update your selection and return to the previous page.

To make a Facet Tree available to users:

1. In a facet folder, click the facet tree’s Functions menu and then click **Properties** > **Availability**.
2. In the **Facet Tree availability** box, enable an option.

   If you enable **Only available in specific locations**, click **Browse Content Server** next to the **Locations** box to select the locations in Content Server that will display your custom facet tree. To make your facet tree available in an additional location, click **Add Location** (+) and repeat the process. To remove a location, click **Remove Location** (−) beside the location that you want to remove.

   Once you have set your **Facet Tree availability** option (and locations, if applicable), click **Update** to save your changes and return to the facet folder.
3. On the Functions menu for your facet tree, click **Properties** and then click **Permissions**.
4. On the **Permissions** page for your custom facet tree, select the user or user group whose permissions you want to edit. On the **Edit User Permissions** page, enable the permissions that you want to assign.
5. Click **Update** to save your changes.
6. Click **Done** to return to the facet folder.

4.2.13 To Select the Facet Tree Location from a Folder

To select the Facet Tree location from a folder:

1. Browse to any folder in Content Server to which you want to apply facet tree configuration. On the Functions menu for that folder, click **Properties**, and then click **Presentation**.
2. If there are trees to display in the **Global Trees** field, click one tree in the list of the facet trees that are available globally.

   You will be taken to the **Availability** tab for the related facet tree in the Facets Volume.
3. If there are trees to display in the **Inherited Trees** field, click one tree in the list of facet trees that are inherited from a parent object.

   You will be taken to the **Availability** tab for the related facet tree in the Facets Volume.
4. Click **Select** to select facet trees from the Facets Volume to add to the list of Local Trees.

   Tip: The **Remove** button is disabled until at least one facet tree is selected in the list of Local Trees. Clicking **Remove** removes the selected facet trees from the list of Local Trees.

5. Click **Update** to save your changes and return to the previous page.

4.2.14 Examples Adding Facets

Example 4-1: To make the Creation Date system attribute available as a content filter throughout Content Server:

1. On the Global Menu bar, from the **Enterprise** menu, select **Facets Volume**.
2. On the **Facets** page, open the **System Default Facets** folder.
3. On the **System Default Facets** page, from the **Add Item** menu, select **Facet**.
4. On the **Add: Facet** page:
   a. In the **Name** field, type “Creation Date”.
   b. In the **Description** field, type “This facet will filter content by Creation Date.”
   c. From the **Data Source** list, choose “Date Created”.
   d. Click **Add**.
5. On the **System Default Facets** folder page, select the **Default System Facets** facet tree.
6. On the **Default System Facets** facet tree page:
   a. Click the plus sign next to **Default System Facets**.
   b. From the list box that appears, select **Creation Date** from the list.
   c. Click **Update**.
7. On the **System Default Facets** folder page, open the **Creation Date** facet.
8. On the **Creation Date** facet page, select the **Specific** tab:
   a. In the **Minimum unique values** field, increase the value to “4”.
   b. Click **Update**.

Example 4-2: To create a facet based on a category's attribute, and make that facet available as a content filter to one folder only:

Note: This example assumes that you have previously created a folder in the Enterprise workspace called “Offices”.

1. You need to first create a category in the Categories Volume. Open the Content Server Administration page.
2. Under the **System Administration** heading, click **Open the Categories Volume**.
3. On the **Content Server Categories** page, from the **Add Item** menu, click **Category**.
4. On the **Add: Category** page, in the **Name** field, type “Office Locations”, and then click **Add**.

5. On the **Content Server Categories** page, from the **Office Locations** category's functions menu, click **Edit**.

   Tip: You can also click the **Office Locations** category link to edit the category.

6. On the **Office Locations** category page, from the **Add Attribute** menu, select **Text: Popup**.
7. On the **Add Attribute to: Office Locations** page:
   a. In the **Name** field, type “Office Location”.
   b. In the **Valid Values** field, type the following entries, each on a new line, without commas or quotes: “Chicago”, “London”, “New York”, “Paris”, “Seattle”, and “Toronto”.
   c. Click **OK**.
8. On the **Office Locations** category page, click **Submit**.
9. On the Global Menu bar, from the **Enterprise** menu, select **Facets Volume**.
10. On the **Facets** page, open the **System Default Facets** folder.
11. On the **System Default Facets** folder page, from the **Add Item** menu, select **Facet Folder**.
12. On the **Add: Facet Folder** page:
    a. In the **Name** field, type “Office Locations”.
    b. In the **Description** field, type “Holds the Facets and the Facet Tree for the Office Locations content filter, displayed on the Enterprise:Offices page.”.
    c. Click **Add**.
13. On the **System Default Facets** folder page, open the **Office Locations** facet folder.
14. On the **Office Locations** folder page, from the **Add Item** menu, select **Facet**.
15. On the **Add: Facet** page:
    a. In the **Name** field, type “Office Location”.
    b. In the **Description** field, type “This facet will filter content by the Office Location category attribute.”
    c. From the **Data Source** list, choose “Category:Office Locations:Office Location”.
    d. Click **Add**.
16. On the **System Default Facets** folder page, from the **Add Item** menu, select **Facet Tree**.
17. On the **Add: Facet Tree** page, in the **Name** field type “Locations”, and then click **Add**.
18. Open the **Locations** facet tree. On the **Locations** facet tree page:
    a. Click the plus sign next to **Locations**.

   b. From the list box that appears, select **Office Location** from the list.

   c. Click **Update**.

19. Open the **Locations** facet tree. On the **Locations** facet tree page:

   a. On the **Availability** tab, select the **Only display in specific locations** button.

   b. In the **Locations** area, click **Browse Content Server...**. Browse to the **Offices** folder that you previously created in the Enterprise workspace.

      Click the **Select** link next to the **Offices** folder.

      The **Locations** field should now read “Enterprise:Offices”.

   c. Click **Update**.

4.2.15 Working with Activity Managers

Users with Knowledge Manager permissions can use the **Activity Manager** item type in the Facets Volume to configure which events will generate an activity feed message.

Each new activity manager is associated to an activity data source. Each activity data source, such as an attribute value, can only have one activity manager. In each activity manager, you can define multiple rules that apply to the associated data source.

When an attribute is modified in Content Server, the system checks whether an activity manager has been defined for that attribute or data source. If an appropriate activity manager exists, the Activity Rules engine will evaluate the rules in that activity manager, in the priority order listed and, if there is a match, will display a customizable activity feed message.

For more information about how to create and work with activity managers, see *OpenText Content Server - Pulse (LLESSOC-UGD)*.

4.3 Working with the Facets Volume Control Panel

The Facets Volume Control Panel provides access to a number of facets-related administrative functions. Some are available to a Knowledge Manager. Others can only be accessed by a Content Server user with the correct usage privilege.

A Knowledge Manager has permission to access the **Configure Facet Count Indicators**, **Configure Global Columns** and **Rebuild Suggest Words** pages. A user with the **Facets and Columns** usage privilege can configure document classes, and a user with the Classic UI Configuration usage privilege can configure the sidebar.

4.3.1 Viewing the Facets Volume Control Panel

The **Facets Volume Control Panel** is available only to administrators and Knowledge Managers. If you are not able to view the **Facets Volume Control Panel**, contact your administrator to request the appropriate permissions.

Use one of the following methods to open the **Facets Volume Control Panel**.

- On the **Enterprise** global menu, click **Facets Volume**. Then, in the Facets Volume, click **Control Panel** on the **Facet** Functions menu.
- If you are an administrator, in the **Server Configuration** section of the Content Server Administration page, click **Configure Facets**, and then click **View Facet Volume**. Then, in the Facets Volume, click **Control Panel** on the **Facet** Functions menu.

4.3.2 Configuring Facet Count Indicators

The facet count can be displayed by either numbers or graphic bar charts. If you take a look at the **Content Filter** sidebar in any workspace, you will note that all facet values have numbers next to them. This is the default setting for Content Server. You can change this setting by displaying the count as graphic bar charts for all users.

To Configure Facet Count Indicators

1. On the **Enterprise** global menu, click **Facets Volume**.
2. On the **Functions** menu of the **Facets** icon, click **Control Panel**.
3. Click **Configure Facet Count Indicators**.
4. Enable the desired **Facet Count Indicator**.
5. Click **Save Changes** to save your changes and return to the **Facets Volume Control Panel** page.

4.3.3 Configuring Global Columns

The global columns page displays two dialog boxes called **Displayed Columns** and **Available Columns**. The **Displayed Columns** dialog box contains the columns that are currently displayed for all users who have permission to view the columns when in Browse View. The **Available Columns** dialog box contains the available columns that can be added to the Browse View for all users.

1. On the **Enterprise** global menu, click **Facets Volume**.
2. On the **Functions** menu of the **Facets** icon, click **Control Panel**.
3. Click **Configure Global Columns**.
4. To the right of the **Available Columns** box are left and right arrows (⇦ and ⇨). Click any column name to select it. To move the highlighted column from

the **Available Columns** box to the **Displayed Columns** box (and display that column to all users), click the right arrow. To move the highlighted column from the **Displayed Columns** box to the **Available Columns** box (and hide that column from all users), click the left arrow.

5. To the right of the **Displayed Columns** box are up and down arrows (⇧ and ⇩) that can be used to move items up and down in display order. The order in which the columns appear, from left to right, in the Content Server Browse View depends on the order in which they appear in the **Displayed Columns** box. The first column listed in the **Displayed Columns** box appears at the far left of the Browse View. Click any column name to select it. To move the column name higher in the list in the **Displayed Columns** box, click the up arrow. To move the highlighted column name lower in the list in the **Displayed Columns** box, click the down arrow.
6. Click **Save Changes** to save your changes and return to the **Facets Volume Control Panel** page.

4.3.4 Rebuilding Suggest Words

Any text-based facet, such as one based on a text category attribute, has an associated set of *Suggest Words*. Suggest Words can be thought of as a collection of word suggestions or an index of facet values, similar to the search index in Content Server.

Content Server searches the word suggestions when you enter characters in the filter box in the Facets **More** dialog. The word suggestions allow Content Server to return both facet values that contain exact matches to what you enter and facet values that are close to what you enter.

It is rarely necessary to use the **Rebuild Suggest Words** utility. However, if OpenText delivers a patch or update that improves Facets functionality, you may need to rebuild the word suggestions to take full advantage of the improvements. OpenText Customer Support may also recommend that you run this utility to address a specific issue.

Tip: The job of rebuilding word suggestions is handled by the Distributed Agent. You can follow its progress on the Distributed Agent Dashboard.

To rebuild Suggest Words

1. On the **Enterprise** global menu, click **Facets Volume**.
2. On the **Functions** menu of the **Facets** icon, click **Control Panel**.
3. Click **Rebuild Suggest Words**.
4. On the **Rebuild Suggest Words** page, click **OK**

Chapter 5

Configuring Virtual Folders

Only the administrator can assign permissions to users or groups which allow them to create Virtual Folders. For information about Virtual Folders, see *OpenText Content Server - Documents and Text Documents (LLESWBD-UGD)*.

5.1 To Assign Users Permissions to Create Virtual Folders

To assign users permissions to create Virtual Folders:

1. On the Content Server Administration page, under the **System Administration** section, click **Administer Object Privileges**.
2. On the **Administer Object Privileges** page, scroll down until you find **Virtual Folder** under the **Object Type** heading.

   By default, the **Create Object Status** is *Restricted*, and the actions available under the **Actions** column are *Edit Restrictions* and *Delete All Restrictions*.
3. Click **Edit Restrictions**. You will now see the **Content Server Group Members Info** page titled **Edit Group: Virtual Folder**.
4. Using the list box and input box on the right, find the person or group to whom you want to assign the permission to create a Virtual Folder.
5. The name of the person or group will appear on the right hand side of the page. Under the **Actions** column, select the **Add to group** check box, then click **Submit**.
6. The individual or group name will now appear in the **Current Group Members** box on the left hand side of the page. Click **Done**.

   Tip: When you want to edit the persons or groups allowed to create Virtual Folders in the future, click **Edit Restrictions** under **Actions** on the **Administer Object Privileges** page.

Chapter 6

Configuring Server Parameters and Settings

On the Configure Server Parameters page, you can modify performance settings, security parameters, basic server parameters, and the Content Server port number. You can also limit access to the Admin account by specifying specific IP addresses, and generate a system report.

6.1 Configuring Basic Server Parameters

You can modify the following settings for Content Server on the **Configure Server Parameters** page:

- **URL Prefix for `/support` Directory**

  The *URL prefix*, also known as the *virtual directory alias*, is mapped to the *support* directory during the installation of Content Server. By default, the *support* directory is located at the root installation level: `/installation_path/support`. It is normally not necessary to change URL prefix; however, if you modify it, you must make the change in Content Server and the web server.

  The default value for the URL prefix is `/img/`.

  Note: You must type a forward slash (/) before and after the URL prefix.

- **Web Administrator Password**

  The Web Administrator password is the password that you use to perform a particularly important administrative action, such as changing the Content Server database. For this reason, the Web Administrator password should only be known by a small set of trusted system administrators.

  It is not the same as the password of the Admin user.

  When Content Server is able to connect to its database and to OTDS, you do not need to use the Content Server Administrator password to access the Content Server Administration page. Instead, your user ID requires a suitable usage privilege (either the **Web Admin** usage privilege or a Business Administration usage privilege). For more information on these and other usage privileges, see "Managing Usage Privileges" on page 344.

  To update the Web Administration password, select **Change Password**, enter the current password, and enter the new password twice. Then click **Save Changes** at the bottom of the page.

- **Site Name**

  The Site Name is the name that is displayed throughout Content Server. The site name should be a simple, user friendly name. The default Site Name is Content Server.

- **Global Content Server**

  You can optionally set up a global Content Server environment. A global Content Server environment is a collection of many Content Server installations in different locations, all connected and communicating with each other. You begin to set up a global Content Server environment by selecting **Enable**.

  Once enabled you need to indicate if this particular Content Server installation will be designated as your primary installation or if you will set this installation as a remote installation of Content Server. You can only designate this installation as a remote installation if you have previously designated another installation of Content Server as your primary. The **Site ID** field requires a unique combination of letters, numbers, and / or symbols that will identify this installation within the global Content Server environment.

- **Administrator E-mail Address**

  If you provide an email address for the Administrator, a link to the address appears on the logon page.

- **Default User Start Page**

  This parameter allows you to select one of the following pages, which is where users are brought to when they first log in:

  - **Enterprise Workspace**, which displays your organization's home page when users sign in.
  - **My Workspace**, which displays each user's Personal Workspace when users sign in.
  - **About Content Server**, which displays the About Content Server page when users sign in.

  Note: If you select **About Content Server**, you need to decide if you want to require that your users login in order to view the page. If you want to require that your users login, select the "**About Content Server**" **Requires Login** check box. This option is disabled by default.

- **Multiple Address Separator for "mailto:" URL**

  You can change the character that is inserted between multiple recipient addresses in message composition windows. If your organization predominately uses Microsoft email applications, you should select **semi-colon** "**;**" for the address separator. For other email applications, you might need to select **comma** "**,**".

- **Enhanced Keyboard Accessibility Mode**

  Enhanced Keyboard Accessibility Mode permits the user interface to be manipulated using keyboard commands. However, certain features that depend on Java, such as the Text Editor, are disabled when Enhanced Keyboard Accessibility Mode is used. This option is disabled by default. When you enable this option, *all* users are required to use this mode.

- **Upload Directory**

The Upload Directory parameter is used to restrict the location from which Content Server accepts Documents for upload. The directory specified in this field must be accessible to both the web server and the Admin server. OpenText recommends that you specify the full path to the directory in this field.

Note: OpenText strongly recommends that you specify an upload directory. Leaving this field blank poses a security risk. It can also prevent you from applying a license file. See "License Management" on page 252.

- **Receive Before Send**

  This setting reduces the amount of time the Server must dedicate to downloading and opening documents. The default setting for **Receive Before Send** is set to `TRUE`. When `ReceiveBeforeSend=TRUE`, the Server's responses are buffered to the web server, which then assumes control of sending the contents to the browser. This allows the available server threads to move on to other requests more quickly. From an end-user perspective, fetching and downloading documents will still take the same amount of time.

- **Socket Timeout**

  Socket Timeout settings govern socket communications on the current Content Server instance. In a clustered installation of Content Server, it is possible to set different network socket timeout values on different Content Server instances.

  Send Timeout sets the maximum time in seconds that Content Server will wait for a receiver response after sending data. The default value is 30 seconds.

  Receive Timeout sets the maximum time in seconds that Content Server will wait for data from a sender. The default value is 2 seconds.

  Set each value to a positive integer greater than zero. To disable either network socket timeout, set its value to `Never`.

- **Server Threads**

  This setting defines the number of threads used by Content Server. The default **Number of Threads** is 8. You may want to increase or decrease the number of threads, depending on:

  - the speed of individual request execution times
  - the amount of capacity needed
  - your usage profile
  - the availability of CPU and RAM resources on your Content Server hardware

  The optimum number of threads depends on the characteristics of your Content Server environment. Items that can be considered include:

  - the number, speed, and architecture (for example, NUMA) of the CPUs
  - the amount of physical memory in your servers
  - the speed of network connections
  - whether storage is local or accessed over the network

It also depends on the usage profile for your Content Server instance (the frequency and variety of the types of user requests).

To determine the number of threads that your server can support, OpenText recommends that you experiment with different thread values. You can measure your results by using Content Server logs and utilities that are available from the operating system. For more information, see *OpenText Content Server - Administering Search (LLESWBS-AGD)*.

Note: Do not set the number of threads higher than the number of connections supported by your RDBMS.

- **Number of Sessions**

  This setting defines the maximum number of user log-in sessions cached on a server thread. The default value of the Number of Sessions is set to 100. When the maximum number of sessions is reached, the oldest user log-in session is dropped. User log-in sessions are cached independently on each thread. When a user returns to a thread after their log-in information has been dropped from the cache, it will take slightly longer to execute their next request. The lower the maximum number of sessions, the less memory the server must dedicate to tracking user log-in sessions on each thread. The larger the number, however, the less often the server will drop user log-in information from the cache. A Server's memory consumption can be large for a system running many threads. You may want to try different values for the maximum number of sessions, depending on how many users are accessing your Content Server system.

6.1.1 To Configure Basic Server Parameters

To configure basic server parameters:

1. In the **Server Configuration** section of the Content Server Administration page, click the **Configure Server Parameters** link.
2. On the **Configure Server Parameters** page, modify any of the server parameters, and then click the **Save Changes** button.

Note: See "Configuring Basic Server Parameters" on page 73.

6.2 Configuring Performance Settings

You can modify the following Content Server performance settings on the **Configure Performance Settings** page:

- "Caching" on page 77
- "Cache Expiration" on page 77
- "File Buffer Size" on page 77
- "Categories Upgrade Batch Processing" on page 78

The **Configure Performance Settings** page is accessible from the Administration page. Click **Server Configuration**, and then click **Configure Performance Settings**.

Tip: In a clustered Content Server environment, the changes that you make on the **Configure Performance Settings** page apply to the Content Server instance that you are accessing, not to the entire Content Server cluster.

Caching

In the **Caching** section, you can decrease the load on Content Server and its database by enabling **Web Caching** and **DAPINode Caching**.

Web Caching

Web caching allows items served by Content Server to be cached by the web server. By default, web caching is not enabled. OpenText recommends that you enable web caching to improve performance.

When web caching is enabled, Content Server validates items in the web server cache. If Content Server confirms that the cache contains the current copy of an item, the item is delivered from the web server cache instead of from Content Server.

DAPINode Caching

DAPINode Caching improves Content Server performance for functions that refer to a CS item (DAPINode) multiple times within a single operation. When **DAPINode Caching** is enabled, Content Server queries the database only once to obtain DAPINode information, then uses cached information thereafter.

DAPINode Caching is enabled by default. OpenText recommends that you leave it enabled, unless Customer Support advises you to disable it for troubleshooting purposes.

Cache Expiration

This setting specifies the number of minutes that Content Server caches data used in various operations. The default is `4320` minutes, which is equal to 72 hours or 3 days. OpenText recommends that you do not change this setting from its default value unless Customer Support advises you to do so.

File Buffer Size

This setting allows you to configure the file buffer size when copying items to and from the External File Store. The file buffer size is specified in bytes. The value must be between 16384 (16 KB) and 2097152 (2 MB). By default, the file buffer size is 524288 bytes (512 KB).

Categories Upgrade Batch Processing

This setting allows you to set the refresh rate of the progress window during batch Category upgrade operations. The default refresh rate is 200 items, which means the progress window will refresh every time 200 Categories are processed.

6.2.1 To Configure Performance Settings

To configure performance settings:

1. On the Content Server Administration page, in the **Server Configuration** section, click **Configure Performance Settings**.
2. On the **Configure Performance Settings** page, do any of the following:
   - Enable or disable web caching.
   - Accept the default cache expiration setting or type a new value, in minutes, in the **Cache Keep Minutes** field.
   - Type the size (in bytes) used for file copy operations in the **File Copy Buffer Size** field.
   - In the **Categories Upgrade Batch Processing** field, type the number of categories that should be processed before the progress window is refreshed.
3. Click **Save Changes**.

6.3 Configuring Security Parameters

You can set options designed to help make Content Server more secure. To access the **Configure Security Parameters** page, from the Content Server Administration page select **Server Configuration**. Click **Configure Security Parameters**.

Note: For additional Content Server security features, see "Limiting Admin Account Log-ins by IP Address" on page 87 and *OpenText Content Server - Notifications Administration (LLESWBN-AGD)*.

HTTP-only Cookies

The **HTTP-only Cookies** section allows you to specify whether the **httpOnly** attribute is added to all Content Server cookies. If enabled, all cookies will be marked with the **httpOnly** attribute. To browsers that support it, this attribute indicates that a cookie should not be made available to scripting. By default, this option is disabled.

Cookie Encryption Key

Content Server creates an authentication cookie using the user's numeric ID and other values that you can specify. The values that you select are necessary to authenticate requests after logging in. The **Cookie Encryption Key** lets you provide a text string for use as the key that encrypts a Content Server authentication cookie.

If a key is not specified in this field, Content Server uses a default key. However, OpenText strongly recommends that you change this value to a unique key.

Data Encryption Key

Content Server also uses a **Data Encryption Key**, which lets you provide a text string for use as the key that encrypts the database administrator's password when it is included in a Content Server request. If a key is not specified in this field, Content Server uses a default key. However, OpenText strongly recommends that you change this value to a unique key.

Cookie Authentication Information

When configuring the authentication cookie, you can include the client's IP address as a value. The **Client IP address** list lets you apply a bit mask when comparing the IP addresses of different requests. The bit mask indicates which portion of the IP address is to be compared; the nonzero elements of the IP address are compared to the IP address placed in the cookie at log-in. For instance, if `255.255.0.0` is selected, only the first two elements will be compared. This makes it possible to verify that requests are coming from the same network, without requiring identical IP addresses. By default, this field is set to `255.255.255.255 (Compare Entire IP Address)`.

If selected, **Enable X-Forwarded-For for Client IP mapping** tells Content Server to read the client IP address from the X-Forwarded-For HTTP header. Otherwise, Content Server reads the IP address from the request. **Trusted Proxy Server List** tells Content Server which X-Forwarded-For proxy IPs to trust.

You can optionally choose to include the **Owner ID** in the authentication cookie. This is the ID of the user who created the user.

You can also set authentication cookies to expire. After the specified interval, Content Server requires a user to log in again. Since Cookie Expiration involves additional interaction with the database, it may have an impact on performance. By default, cookies are set to expire 30 minutes after the last action is performed.

Log-in Cookie Expiration Date

You can set the cookie expiration date to manage cookies for the Content Server log-in page. This parameter controls the language display when users have multiple language packs installed. A cookie on the Content Server log-in page remembers a user’s language selection until they are authenticated, after which it uses their preferred language.

The cookie expiration date is calculated based on the date and time value of a user's computer, not the date and time of Content Server. The number of days must be a positive integer between 1 and 999. By default, the log-in cookies are set to expire after 8 days.

Log-in Connection Policies

This section helps secure Content Server against repeated failed user logon attempts, multiple concurrent sessions being opened by the same user, and cross-site forgery requests.

- Enabling **Disable simultaneous sessions from multiple machines** prevents users from simultaneously accessing Content Server from more than one computer. If you enable this feature, users can sign in to Content Server from one computer, but if they sign in a second time from another computer, the first Content Server session is terminated.

  In the **except for hosts** field, you can provide a comma-delimited list of IP addresses for any computers to which this feature does not apply. Also, you can specify a single * wildcard character to indicate multiple computers. For example, a valid entry is: `123.45.*,192.*,123.99.2.51`. By default, this option is disabled.
- The **Allow log-in via HTTP GET request** setting, if enabled, grants access to the Content Server authentication methods from HTTP Get requests. The LLCookie is returned upon successful authentication. This setting may be required for integration with specific (older) external applications. This option is disabled by default.
- The **Require secure request token** setting, if enabled, helps to prevent cross-site request forgery: an attack whereby a user unknowingly initiates an action that takes place in software to which the user has already logged on. The secure request token is a value that is shared from the server to the browser when the user performs certain actions. This value must accompany requests for other actions. If the value is not present, the requested action is invalid. This option is disabled by default.

Password Retries

This section defines the numbers of times an incorrect password can entered by a Content Server **Web Administrator** and **Admin** before the log-in is disabled, and whether to send an e-mail to the Administrator. By default, these options are enabled.

The login policies include options to alert administrators of policy exceptions by e-mail, as specified on the **Configure Server Parameters** page. If the Administrator e-mail address is not specified, the notification message is not sent. For more information about specifying the Administrator e-mail address, see "Configuring Basic Server Parameters" on page 73.

- **Web Administrator**

  If too many incorrect password attempts are made to enter the Web Administrator password, the Web Administrator password entry can be disabled for a period of time to reduce exposure to possible brute-force password guessing.

  - **Disable log-in when password incorrect**, which enables you to specify actions when a Web Administrator's log-in fails.
  - **Number of allowable log-in attempts** before the account is disabled. By default, this setting is enabled, and the number of allowed failed log-in attempts is set to **5**.
  - **Number of minutes log-in is disabled**, which allows you to specify how long the Web Administrator must wait before attempting to log-in again. By default, this setting is enabled, and the number of minutes is set to **5**.
  - **Send e-mail to the Administrator when log-in is disabled**, which allows you to specify the Content Server Administrator should receive an email whenever the specified number of log-in attempts is exceeded.

- **Admin**

  The Admin account is essential, and cannot be disabled without impacting the system. This policy allows you to alert Admins to the possibility that someone is trying to guess the password.

  Beginning with Content Server 16.0, this functionality is now configured in Directory Services. It applies to authentication mechanisms that access Content Server directly instead of using the Directory Services (OTDS) Log-in page. For failed log-in attempts in OTDS, please refer to the *OpenText Directory Services - Installation and Administration Guide (OTDS-IWC)*.

  - **Send e-mail to Administrator on too many password failures**, which allows you to specify whether the Content Server Administrator should receive an email whenever the specified number of log-in attempts is exceeded.
  - **Password failure threshold**, which allows you to specify the number of times an Admin can attempt to log in to Content Server before an email is sent. By default, this setting is enabled, and the number of allowed failed log-in attempts is set to 5.

    Note: The disable log-in feature does not apply to the Content Server Admin account. You can protect the Content Server Admin account by allowing only certain client IP addresses access. For more information about limiting Content Server Admin account log-in attempts by IP address, see "Limiting Admin Account Log-ins by IP Address" on page 87.

Frame Embedding

You can optionally choose to prevent request handlers from being embedded in external frames by selecting the **Prevent request** option. By default, this option is selected.

Request Argument Filtering

When **Request Argument Filtering** is enabled, all client requests to Content Server are compared with the values in the **Filter String** field. By default, these fields are blank. If any matches are found, the request is rejected.

The filter list is delimited by a separator that you specify. For example, if you use a comma (`,`) as the separator, type three filters as:

`<Filter_A>`, *`<Filter_B>`*, *`<Filter_C>`*

The separator is configurable to prevent conflicts with desired filters. For example, if you want to use a backslash as the separator, type:

`<Filter_A>`\ *`<Filter_B>`*\ *`<Filter_C>`*

Secure Request Token Expiration

The **Secure Request Token Expiration** field is part of an enhanced security framework that allows requests to access authentication token (cookie) generation and verification functionality. A token can be passed between sequential requests and ensure that appropriate security checks occur. The default setting is set to timeout after 300 seconds.

Content Server Client Hosts

The **Content Server Client Hosts** field contains the IP addresses of servers from which requests are to be accepted. By default, the field is blank, and all client connections are accepted.

Trusted Referring Websites

The **Trusted Referring Websites** parameter is a security measure used to prevent other users from exploiting your website. The sites contained in this list appear in an HTTP Referrer header, which validates HTTP requests coming from another website. If a request comes from an unauthorized website, the action will not be permitted, and an error message is displayed.

If you are adding multiple web addresses, ensure each address appears on a separate line. For example:

```
company.com
sub.company.com
*.company.com
```

Beginning with Content Server 16, Update 2017-03, changes were made to reduce vulnerabilities, and to improve the security level for customer's authorized websites.

Important

If your existing Content Server installation has URL entries such as `http://domain.company.com` defined in your valid list of referrers, you will need to change the URL entry to conform to these new requirements.

OpenText strongly recommends you restrict access to some websites until your settings are updated.

The protocol, HTTP or HTTPS, is ignored when checking the defined list of referrers against the incoming request.

The valid list of domains is right anchored by default. For example, if `http://domain.com` is defined, `http://domain.company.projects.com` will not be accepted.

Use asterisks (`*`) as wildcards to indicate one or more subdomains. Use the `*.` prefix for all subdomains. For example, `*.company.com` will allow:
`http://www.company.com`
`http://intranet.company.com`
`https://subdomain.othersub.company.com`
However, a listing `company.com` will allow `http://company.com` or `https://company.com`.

An asterisk is ***not*** an all-purpose wildcard. For example, the entry `fred.*.company.com` is ***not*** a valid entry, nor is `company.*`, or `*company.com`.

A percent sign (`%`) cannot be used as a stemming operator in an entry. Any `HTTP_REFERER` string having a `%` in the domain portion cannot be matched.

Port numbers, for example, `http://domain.company.com:8080` are ignored when checking the list against the request.

Using IPv6 URI (Uniform Resource Identifier) is not supported.

All addresses entered are evaluated to prevent invalid entries being saved to the `opentext.ini` file, and to allow for system feedback to the administrator.

Note: For Enterprise Process Services Integration, you must enter the **Trusted Referring Websites** parameter in the following format: *`http://<PW Server>`*, where *<PW Server>* is the computer where Process Workplace (the web server part of Enterprise Process Services) is running.

Beginning with Content Server 16, Update 2018-03, you can add sites without a fully qualified domain name (FQDN), or an absolute domain name, by adding entries to the `opentext.ini` file. If multiple hostname labels are specified, for example, `xxxx.yyyyy`, the rightmost label is subject to top level domain restrictions `[A-Za-z]{2,63}`.

Trusted Cross Domains

The **Trusted Cross Domains** field allows you to manage Content Server and third party web application integrations. You register the *`<key>`* `;` *`<target>`* pair where *`<key>`* is a value to be passed in as a URL parameter and will perform the registration lookup and *`<target>`* is a registered URL path to the target resource (third party web application).

If you are adding multiple HTTP web addresses, ensure each address appears on a separate line. For example, `pw;http://<my-server>/pw/client/csbrowse.htm`

Note: For Enterprise Process Services Integration, you must enter the **Trusted Cross Domains** parameter in the following format: *`pw;http://<PW server>/pw/client/csbrowse.htm`*, where *<PW Server>* is the computer where Process Workplace (the web server part of Enterprise Process Services) is running.

6.3.1 To Configure Security Parameters

To configure security parameters:

1. In the **Server Configuration** section of the Content Server Administration page, click the **Configure Security Parameters** link.
2. On the **Configure Security Parameters** page, in the **HTTP-only Cookies** field, click one of the following buttons:
   - **Enable**, to include the **httpOnly** attribute when setting authentication cookies.
   - **Disable**, to exclude the **httpOnly** attribute from authentication cookies.
3. In the **Cookie Encryption Key** field, type an encryption key, as a text string more than one character in length.
4. In the **Data Encryption Key** field, type an encryption key, as a text string more than one character in length.

   Warning

   Although Content Server uses a default key for encryption if the **Cookie Encryption** and **Data Encryption** fields are left blank, OpenText strongly recommends that you enter unique keys.
5. In the **Cookie Authentication Information** area, do the following:
   - To use the client IP address as part of the authentication cookie, click a value in the **Client IP address** list that represents the portion of the client IP address to be compared.
   - To enable *X-Forwarded-For* for client IP mapping, select the associated **Enable** box.
   - In the **Trusted Proxy Server List** field, type the proxy server addresses that you want to register as trusted.
   - Select the **Owner ID** check box to choose user attributes for inclusion in the authentication cookie.
   - Click one of the following radio buttons, and, if applicable, type an integer for the number of minutes, to manage the cookie expiration interval:
     - **Never Expire**
     - **Expire <***number_of_minutes***> minutes after last request**
     - **Expire <***number_of_minutes***> minutes after last login**

6. In the **Log-in Cookie Expiration Date** field, select one of the following radio buttons, and, if applicable, type an integer for the number of days, to specify how long the current cookie authentication is valid:

   - **Never Expire**
   - **Expires in <*number_of_days*> day(s)**

7. In the **Log-in Connection Policies** area:

   - Select the **Disable simultaneous sessions from multiple machines** check box to disable a user session if the user logs in to Content Server on more than one computer.

     Specify the list of computers to which this feature does not apply in the **except for hosts** field.

   - Select the **Allow log-in via HTTP GET request** check box to enable users to sign in through the *HTTP Get request*. This option is disabled by default.

8. In the **Password Retries** area:

   - For **Web Administrator**:

     - Select the **Disable log-in when password incorrect** check box to specify actions when a user's log-in fails.
     - Specify the **Number of allowable log-in attempts** before the account is disabled.
     - Specify the **Number of minutes log-in is disabled** before the Web Administrator can attempt to log-in again.
     - Select the **Send e-mail to the Administrator when log-in is disabled** check box so the Content Server Administrator will receive an email whenever the specified number of log-in attempts is exceeded.

   - For **Admin**:

     - Select the **Send e-mail to the Administrator when log-in is disabled** check box so the Content Server Administrator will receive an email whenever the specified number of log-in attempts is exceeded.
     - Specify the **Password failure threshold** for the number of times an Admin can attempt to log in to Content Server before an email is sent.

9. In the **Frame Embedding** field, clear the checkbox to allow request handlers to be embedded in external frames.

10. In the **Request Argument Filtering** area, do the following to enable request-argument filtering:

    - In the **Filter String** field, type the strings that you want to exclude from a Content Server request. For example, to prevent a script from being saved to Content Server as part of a Text Document, type: *`<Script>`*

> **Note:** Avoid using a common URL character, such as a period (`.`) or slash (`/`), as a filter.

- In the **Separator Character** field, type the character that is to be treated as a *separator* between elements in the filter list, not part of the element itself.

11. In the **Secure Request Token Expiration** field, click one of the following buttons:

    - **Never Timeout**
    - **Timeout <***number_of_seconds***> seconds after preceding request**, then type an integer for the number of seconds before a timeout occurs.

12. In the **Content Server Client Hosts** field, specify the servers from which client requests are to be accepted. Multiple IP addresses must be separated by commas. Requests originating from servers not on this list are rejected.

    > **Note:** The list of client hosts may also be used by the other Content Server modules. Do not delete or change any existing IP addresses that may appear in this field. Doing so could adversely affect your system.

13. In the **Trusted Referring Websites** field, type the HTTP web addresses that you want to be authorized. If you are adding multiple HTTP web addresses, ensure each address appears on a separate line.

14. Do the following in the **Document Functions** area:

    - Click the Open function's **Enabled** button to allow users to open documents.
    - Click the View as Web Page function's **Enabled** button to allow users to view documents as web pages.

15. In the **Trusted Cross Domains** field, enter the following *`<key>`*; *`<target>`* pair where *`<key>`* is a unique case-sensitive alpha-numeric tag used to register the third party web application and *`<target>`* is a registered URL path to the target resource.

16. Click **Save Changes**.

17. The **Restart Content Server** page appears. Click **Restart** to restart automatically (or click **Continue** if you prefer to restart Content Server using the operating system). Restart your web application server, if applicable. When the **Restart Successful** message appears, click **Continue** to return to the Content Server Administration page.

6.4 Specifying the Server Port Number

The port on which the Server listens is specified during the installation process. Do not modify it, unless a port conflict arises that cannot be resolved in any other way.

6.4.1 To Specify the Server Port Number

To specify the Server port number:

1. Click **Specify Server Port** in the **Server Configuration** section on the Administration page.
2. Type an unused port number between 1,025 and 65,535, on which you want Content Server to listen in the **Port Number** field.

   On Linux, only the root user has the privileges necessary to run processes on port numbers 1 to 1,024. For this reason, OpenText recommends that you do not use this range of port numbers for Content Server.
3. In the **Family Hint** field, select the address family on which Content Server should listen for requests.
4. Click **Save Changes**. An error message appears, indicating that the Server did not respond.
5. Restart Content Server and then refresh your browser. The **Restart Content Server** page appears.
6. On the **Restart Content Server** page, click **Continue** (because you have already used the operating system to restart Content Server).

6.5 Limiting Admin Account Log-ins by IP Address

By default, you can log onto Content Server as the Admin user from any IP address that has access to your organization's computer network. However, as a security measure, you can restrict Admin’s ability to log on to Content Server. You can configure Content Server to prevent the Admin user from logging on unless the logon attempt originates from an approved IP address.

The values that you add to the **Allowed IP Addresses** field can include an explicit IP address or an IP address that contains an asterisk (*) that acts as a wildcard to replace portions of the address. Using asterisks lets you include a group of computers that have portions of their IP address in common.

! **Important**

If you have installed OpenText™ Directory Services, the settings you make on this page also prevent the otadmin@otds.admin user from logging on from an unapproved IP address.

6.5.1 To Limit Admin Account Log-ins by IP Address

To limit the Admin account log-in by IP address:

1. In the **Server Configuration** section of the Administration page, click **Limit the Admin Account Log-in**.
2. On the **Limit the Admin Account Log-in** page, do one of the following:
   - To add an IP address, type it in the provided field, and then click **Add IP Address**.
   - To delete an IP address, click the address in the associated list, and then click **Delete**.

   Note: To allow Admin to log on locally on the Content Server computer, you must permit logon from the IP address `127.0.0.1`.
3. Click **OK**.
4. Restart Content Server and, if applicable, the web application server.

6.6 Configuring SLD Registration

System Landscape Directory (SLD) is a central repository of information about all of the products or modules installed on NetWeaver. You can use the SLD Registration page in Content Server to generate a SLD file with Content Server's information. Once the SLD file is generated, NetWeaver uses the information to add Content Server to its SLD.

6.6.1 To Configure SLD Registration

To configure SLD Registration:

1. In the **Server Configuration** section of the Content Server Administration page, click the **SLD Registration** link.
2. On the SLD Registration page, select the type of file you want to generate in the **Type of file** drop-down list, and then click the **Generate** button.
3. Click the **Generate** button.

6.7 Generating a System Report

A *System Report* contains extensive details about your Content Server system. There are two types of System Reports: the *Lite System Report* and the *Full System Report*. Each report contains information about the following:

- System
- Licensing of Content Server and installed modules
- Current database and database server
- Application (number of Workflows, Categories, and Additional Node Attributes)
- Users and groups
- Node types (subtypes)
- Storage providers
- Outdated date attributes
- OSpaces
- Patches applied, skipped and overwritten
- Request handlers
- Custom modules
- Custom OSpaces
- AgentSchedule database table
- LLSystemdata database table
- KIni database table
- opentext.ini contents
- Install directory (full listing of all application files, including Modified date and size)
- Additional customized reports

The Full System Report also contains information about the following:

- Node versions
- Additional database properties
- Content Server database tables
- Content Server database table columns
- Content Server database indexes
- Content Server database triggers
- Content Server database stored procedures
- Content Server Tablespace Information (Oracle only)

- Document MIME Types

The generated report is a text document, called `sysreport.txt`, that resides in the `logs` folder of your Content Server installation. When you finish generating a System Report, its location appears as a link beside **File Path** on the **Content Server System Report** page. Click the link to open the report.

If a System Report has previously been generated, a link to the most recent system report appears at the top of the **Content Server System Report** page. To obtain an up-to-date System Report, click **Generate** to create a new one.

6.7.1 To Generate a System Report

To generate a System Report:

1. In the **Server Configuration** section on the Administration page, click **System Report**.
2. On the **Content Server System Report** page, enable **Lite System Report** or **Full System Report**.
3. Click **Generate**.

6.8 Modifying System Configuration Files

Some system configuration settings cannot be made from the Content Server Administration page and instead require you to edit a configuration file. In most cases, the file that you must edit is the `opentext.ini` file, which is located in the *`<Content_Server_home>`*`/config/` folder. The `mime.types` and `mime.gifs` files, located in the same folder, are other files that you may need to modify to implement desired behaviors in Content Server. If you need to modify search settings in a configuration file, it is likely that you will edit the `otadmin.ini` file.

! **Important**
Always stop Content Server before you edit a Content Server configuration file. Editing a configuration file while Content Server is running can result in corruption of the configuration file and prevent Content Server from running properly. If you are editing a configuration file that affects the Admin server or Cluster Management, stop the Admin Server or the Cluster Agent.

After you edit a Content Server configuration file, restart Content Server and, if applicable, the Admin server or the Cluster Agent, and your application server, so that your changes to take effect.

6.8.1 To Modify System Configuration Files

To modify a system configuration file:

1. Log on to the primary Content Server host as the operating-system user that the servers run as.
2. Stop Content Server. If applicable, stop the Admin server or the Cluster Agent.
3. Open the appropriate file in a text editor.
4. Edit the file as needed to implement the change.
5. Save and close the file.
6. Restart Content Server and, if applicable, the Admin server, the Cluster Agent, and your web application server.

Chapter 7

Understanding the opentext.ini File

The `opentext.ini` file is the main Content Server configuration file for both primary and secondary Content Server installations. It contains such settings as database connection options, paths to files, date formats, debugging options, and logging options.

The `opentext.ini` file is created during the Content Server installation process. At that time, the default options are set and many settings are configured dynamically. Some settings, such as the encoded Administrator's password and Notification settings, are changed by Content Server as necessary.

Most of the settings that appear in the `opentext.ini` file can be changed on the Content Server Administration page, but some settings must be changed by manually editing the `opentext.ini` file in a text editor. For more information, see "Modifying the opentext.ini File" on page 93.

7.1 Modifying the opentext.ini File

Although most Content Server configurations can be performed on the Content Server Administration page, some Content Server configurations must be implemented by editing the `opentext.ini` file.

Note: If you can modify Content Server parameters either on the the Content Server Administration page or in the `opentext.ini` file, it is preferable to use the Administration page. You should manually edit the `opentext.ini` file only if you are instructed to do so by:

- an instruction in a Content Server document, such as this Help or the *OpenText Content Server - Installation Guide (LLESCOR-IGD)*
- OpenText Customer Support

The `opentext.ini` file is located in the *`<Content_Server_home>`*`/config/` folder, where *`<Content_Server_home>`* is the root of your Content Server installation. It is organized according to the standard Windows INI-file structure. It is composed of sections, each of which is headed by a section name in square brackets. Each section contains zero or more properties. These properties are in the form *`<name>`*`=`*`<value>`*. The order of the sections is not important. Section titles and name strings are not case-sensitive, but value strings are.

Settings in the `opentext.ini` file normally affect only a single instance of Content Server. In a Content Server cluster, any changes that you make to the `opentext.ini` file must typically be made on the `opentext.ini` file of every node in your cluster. In contrast, the settings that appear on the Content Server Administration page typically affect every Content Server instance in your cluster, so you only need to change a setting there once.

Important

You must stop Content Server before you edit the `opentext.ini` file. Make any changes that are required, and then restart Content Server (and, if applicable, your web application server) to put the changes into effect. In some cases, you must also restart the Admin server.

For information about modifying other system configuration files, see “Modifying System Configuration Files” on page 90.

7.2 Node Type Number to Name Mappings

Each node type that is defined in Content Server is identified by its *subtype*. A subtype is a unique, identifying integer that is stored in the node type's LLNode and WebNode objects.

To see the complete node type number to name mappings, run a system report and view the “Node Types” section.

The following table shows some of the common node types for a standard Content Server installation. If you install optional modules, your system may have additional node types that are not listed here. Also, customizations to Content Server can create custom node types that are not listed.

Node Type ID	Node Type Description
0	Folder
1	Alias
2	Generation
128	WFMap
130	Topic
131	Category
132	Category Folder
133	VolCategories
134	Reply
136	CompoundDoc
137	VolRelease
138	Release

Node Type ID	Node Type Description
139	Revision
140	URL
141	VolLibrary
142	VolWorkbin
143	VolDiscussion
144	Document
146	CustomView
148	VolSystem
154	WorkflowAttachments
161	VolWorkflow
162	VolEditWorkflow
180	VolDomainWorkspace
190	WFStatusNode
201	ProjectVol
202	Project
204	TaskList
205	TaskGroup
206	Task
207	Channel
208	News
209	ChannelVol
210	TaskListVol
211	VolReports
212	TaskMilestone
215	Discussion
218	Poll
257	OTCIndexObj
258	SearchBroker
259	LibraryExtractor
260	Proxy
268	TemplateFolder
269	SearchManager
270	Data Flow Manager

Node Type ID	Node Type Description
271	Process
272	LibraryObj
273	Merge
275	Slice Folder
276	DataSourceFolder
277	DirWalker
278	SearchReport
281	IndexUpdate
282	HTMLConversion
285	XMLActivatorProd
286	XMLActivatorCon
290	BackupManager
291	BackupProcess
292	SearchTemplate
293	Importer
294	2WayTee
299	Report
335	DTDLLNode
336	VolDTD
368	IndexEngine
369	SearchEngine
370	PartitionMap
371	Partition
380	ProspectorQueries
384	Prospector
387	ProspectorSnapshot
402	VolDeletedDoc
480	Appearance
481	AppearancesVolume
482	GlobalAppearance
483	AppearanceFolder
484	VolumeFolder
541	ItemTemplateVol

Node Type ID	Node Type Description
542	ItemTemplateVolFolder
543	ProjectTemplate
903	FacetTree
904	Facet
905	FacetFolder

7.3 Opentext.ini File Settings Reference

This section of the Admin Help describes `opentext.ini` file settings. The settings are listed under the section name that they occur under, and the section names are sorted alphabetically. Only the settings that are present in a default installation of Content Server are covered in this section. For `opentext.ini` file settings that govern the behavior of optional, custom, and third-party modules, see the documentation that accompanies these products.

7.3.1 [AFORM]

The `[AFORM]` section allows you to add a setting to troubleshoot PDF forms in Content Server. Add this section, with the setting below, to set Content Server to create form debugging files.

wantDebug

- **Description:**

  Instructs Content Server to create form debug files that describe the form data retrieval from PDF forms.

- **Syntax:**

  ```
  wantDebug=MORE
  ```

- **Values:**

  `MORE`

7.3.2 [AdminHelpMap]

The `[AdminHelpMap]` section contains mappings that enable context-sensitive online help for items available only to the Administrator or users with system administration rights. Help mappings for user functionality are found in the `[HelpMap]` section of `opentext.ini`. For more information, see “[HelpMap]” on page 163.

A help mapping creates a link between a keyword that identifies a page of the Content Server interface, for example, the Administration page, and the name of an HTML online help page.

! **Important**
OpenText recommends that you do not change the default mappings for [AdminHelpMap] in the `opentext.ini` file.

7.3.3 [agents]

This section contains proprietary OpenText information.

! **Important**
OpenText recommends that you do not change any of the options in this section.

7.3.4 [Attributes]

The `[Attributes]` section controls options for implementing complex attributes.

AttributeMaxRows

- **Description:**

  Sets the maximum number of repeating values allowed in the user interface.

- **Syntax:**

  AttributeMaxRows=50

- **Values:**

  An integer between `1` and `100`. The default value is `50`.

7.3.5 [BaseHref]

The `[BaseHref]` section controls options for setting the *BASE HREF* value in an HTML page that includes a custom view.

Protocol

- **Description:**

  One of either *http* or *https*.

- **Syntax:**

  ```
  Protocol=http
  ```

Host

- **Description:**

  The hostname of the server to include in the BASE HREF URL.

- **Syntax:**

  ```
  Host=myhostname
  ```

Port

- **Description:**

  The port of the web server used in the BASE HREF URL.

- **Syntax:**

  ```
  Port=3000
  ```

- **Values:**

  A positive integer.

7.3.6 [Catalog]

The `[Catalog]` section controls the default behavior of the Catalog display view for workspaces.

NGrandChildren

- **Description:**

  Defines the number of children to display in catalog view.

- **Syntax:**

  ```
  NGrandChildren=6
  ```

- **Values:**

  An integer greater than, or equal to, zero. The default value is `6`.

7.3.7 [cgi_logs]

Contains settings that affect the generation of Content Server web server client logs.

OpenText recommends that you modify the values in this section on the **Configure Log Settings** page, rather than by editing the `opentext.ini` file. For more information, see “Configuring Log Settings” on page 33.

logLevel

- **Description:**

  Sets the level of logging. You can specify a level of `0` (no logging), `1` (warning messages), `2` (info messages) or `3` (debug messages).

- **Syntax:**

  ```
  logLevel=3
  ```

- **Values:**

  A number from 0 to 3. The default value is `0`.

logPath

- **Description:**

  The file path where the web server client logs are generated.

- **Syntax:**

  `logPath=.\logs\cgi_logs\`

- **Values:**

  A file path that is relative to the <*Content_Server_home*> folder, or an absolute file path. The default value is `.\logs\cgi_logs\`.

enableRollingLogs

- **Description:**

  Enables rolling log files.

- **Syntax:**

  `enableRollingLogs=FALSE`

- **Values:**

  `TRUE` or `FALSE`. The default value is `FALSE`.

maxBackupIndex

- **Description:**

  If `enableRollingLogs=TRUE`, the number of rolling log files to keep before overwriting the oldest existing log file.

- **Syntax:**

  `maxBackupIndex=10`

- **Values:**

  A number between `1` and `13`. The default value is `10`.

maxFileSize

- **Description:**

  If `enableRollingLogs=TRUE`, the maximum size of a log file in megabytes. When a log file reaches its `maxFileSize`, Content Server creates a new log file and starts writing to it.

- **Example:**

  `maxFileSize=50`

- **Values:**

  A positive integer. The default value is `50`.

enableCompression

- **Description:**

  If `enableRollingLogs=TRUE`, causes completed log files to be compressed.
- **Syntax:**

  `enableCompression=FALSE`
- **Values:**

  `TRUE` or `FALSE`. The default value is `FALSE`.

enableBuffering

- **Description:**

  Buffer log file output in memory before writing to the log file, to enable faster performance at the cost of some risk of output not being written to a log file.
- **Syntax:**

  `enableBuffering=FALSE`
- **Values:**

  `TRUE` or `FALSE`. The default value is `FALSE`.

bufferSize

- **Description:**

  If `enableBuffering=TRUE`, the size in KB of the memory buffer used to hold log file output.
- **Syntax:**

  `bufferSize=10`
- **Values:**

  A positive integer. The default value is `10`.

7.3.8 [chicklet]

The `[chicklet]` section contains the image file that appears in the masthead in the upper, right-hand corner. You can replace the default image, , with your own organization's image file.

For optimum viewing, your image file should have the following properties:

Property	Value
Decoded size in bytes	7064
Image dimensions in pixels	83 x 30

Property	Value
Color	24-bit RGB true color
Colormap	none
Transparency	no

The image file resides in the *<Content_Server_home>*/support directory, where <*Content_Server_home*> is the root of your Content Server installation. If you change the image file, restart Content Server and, if applicable, the web application server.

7.3.9 [Client]

The [Client] section of the opentext.ini file contains options specific to the configuration of Content Server clients. The following Content Server Administration page describes changes you can make to the [Client] section:

- "Configuring Performance Settings" on page 76

This page contains information about the following parameters:

• "ErrorRedirectURL" on page 102 • "ErrorStatus" on page 102 • "MaxHeaderBytes" on page 103	• "ReceiveBeforeSend" on page 103 • "StrictClientParse" on page 103

ErrorRedirectURL

- **Description:**

  A URL to which users are redirected when attempting to log in to Content Server while the server is not running, passing the information displayed on the default page in a CGI variable called errid. Servlet client connections are not redirected.

  By default, this entry is not displayed in the opentext.ini file until it is set, which is equivalent to ErrorRedirectURL=.

- **Syntax:**

  ```
  ErrorRedirectURL=http://www.opentext.com
  ```

- **Values:**

  Any valid URL.

ErrorStatus

- **Description:**

  When the server is not running, this code is sent in the HTTP header.

  By default, this entry is not displayed in the opentext.ini file until it is set, which is equivalent to ErrorStatus=.

- **Syntax:**

  ```
  ErrorStatus=503
  ```

- **Values:**

  A valid HTTP code.

MaxHeaderBytes

- **Description:**

  Sets the maximum size of HTTP headers in bytes. Content Server uses this setting to limit the size of the HTTP header. If the actual size of HTTP header sent by Content Server is larger than this limit (if the HTTP header contains a large cookie, for example), the browser might be unable to render Content Server webpages.

  By default, this entry is not displayed in the `opentext.ini` file until it is set, which is equivalent to `MaxHeaderBytes=2000`.

- **Syntax:**

  ```
  MaxHeaderBytes=2000
  ```

- **Values:**

  A positive integer representing the maximum size of headers in bytes. The default value is `2000`.

ReceiveBeforeSend

- **Description:**

  When set to `TRUE`, it hands responsibility for the downloading of files to the web server. This frees up Content Server threads more quickly to perform other functions.

  OpenText recommends that you only modify this value using the **Configure Performance Settings** page, rather than edit the `opentext.ini` file directly. For more information, see “Receive before Send” in “Configuring Performance Settings” on page 76.

- **Syntax:**

  ```
  ReceiveBeforeSend=FALSE
  ```

- **Values:**

  `TRUE` or `FALSE`. The default value is `FALSE`.

  Setting this parameter to `TRUE` hands responsibility for the downloading of files to the web server.

StrictClientParse

- **Description:**

  Requires clients to be strict when parsing an input web request. It will produce errors instead of passing on incomplete requests to the server.

- **Syntax:**

```
StrictClientParse=TRUE
```

- **Values:**

  TRUE or FALSE. The default value is TRUE.

  Setting this parameter to FALSE does not require the client to be strict when parsing an input web request.

7.3.10 [connect_logs]

Contains settings that affect the generation of Content Server SQL connect logs.

OpenText recommends that you modify the values in this section on the **Configure Log Settings** page, rather than by editing the `opentext.ini` file. For more information, see “Configuring Log Settings” on page 33.

logLevel

- **Description:**

  Sets the level of logging. You can specify a level of `0` (no logging), `1` (warning messages), `2` (info messages) or `3` (debug messages).

- **Syntax:**

  ```
  logLevel=3
  ```

- **Values:**

  A number from 0 to 3. The default value is `0`.

logPath

- **Description:**

  The file path where the connect logs are generated.

- **Syntax:**

  ```
  logPath=.\logs\connect_logs\
  ```

- **Values:**

  A file path that is relative to the <*Content_Server_home*> folder, or an absolute file path. The default value is `.\logs\connect_logs\`.

enableRollingLogs

- **Description:**

  Enables rolling log files.

- **Syntax:**

  ```
  enableRollingLogs=FALSE
  ```

- **Values:**

  TRUE or FALSE. The default value is FALSE.

maxBackupIndex

- **Description:**

  If `enableRollingLogs=TRUE`, the number of rolling log files to keep before overwriting the oldest existing log file.

- **Syntax:**

  ```
  maxBackupIndex=10
  ```

- **Values:**

  A number between `1` and `13`. The default value is `10`.

maxFileSize

- **Description:**

  If `enableRollingLogs=TRUE`, the maximum size of a log file in megabytes. When a log file reaches its `maxFileSize`, Content Server creates a new log file and starts writing to it.

- **Example:**

  ```
  maxFileSize=50
  ```

- **Values:**

  A positive integer. The default value is `50`.

enableCompression

- **Description:**

  If `enableRollingLogs=TRUE`, causes completed log files to be compressed.

- **Syntax:**

  ```
  enableCompression=FALSE
  ```

- **Values:**

  `TRUE` or `FALSE`. The default value is `FALSE`.

enableBuffering

- **Description:**

  Buffer log file output in memory before writing to the log file, to enable faster performance at the cost of some risk of output not being written to a log file.

- **Syntax:**

  ```
  enableBuffering=FALSE
  ```

- **Values:**

  `TRUE` or `FALSE`. The default value is `FALSE`.

bufferSize

- **Description:**

  If `enableBuffering=TRUE`, the size in KB of the memory buffer used to hold log file output.

- **Syntax:**

  ```
  bufferSize=10
  ```

- **Values:**

  A positive integer. The default value is `10`.

7.3.11 [dateformats]

The `[dateformats]` section controls how Content Server deals with dates and times. To modify these parameters, OpenText recommends that you use the **Administer Date/Time** page, rather than edit the `opentext.ini` file directly. For more information, see "Setting Date and Time Formats" on page 30.

This page contains information about the following parameters:

• "InputDateMinYear" on page 106 • "InputDateMaxYear" on page 106	• "TwoDigitYears" on page 107 • "WantTimeZone" on page 107	• "SeparateCentury" on page 107

InputDateMinYear

- **Description:**

  Limits how many years in the past users can choose from, in the lists provided to users.

- **Syntax:**

  ```
  InputDateMinYear=1990
  ```

- **Values:**

  A positive integer. The default value is `1990`.

  You can set this value as low as you like; there is no numeric limit. However, it is best to set it to something that makes sense in the display.

InputDateMaxYear

- **Description:**

  Limits how many years in the future users can choose from, in the lists provided to users.

- **Syntax:**

  ```
  InputDateMaxYear=2027
  ```

- **Values:**

  A positive integer whose limit is 400,000. The default value is `2027`.

  It is best to set the value of this parameter to something that makes sense in the display. A very large setting causes pages to render more slowly and can have a noticeable effect on your performance.

TwoDigitYears

- **Description:**

  Indicates whether Content Server displays years as two-digit numbers or four-digit numbers.

- **Syntax:**

  ```
  TwoDigitYears=FALSE
  ```

- **Values:**

  `TRUE` or `FALSE`. The default value is `FALSE`.

  Setting this parameter to `TRUE` displays the year 2002 as `02`. If you leave the default value, `FALSE`, the year 2002 is displayed as `2002`.

WantTimeZone

- **Description:**

  Indicates whether the Time Zone Offset feature is enabled.

- **Syntax:**

  ```
  WantTimeZone=FALSE
  ```

- **Values:**

  `TRUE` or `FALSE`. The default value is `FALSE`.

  Setting this parameter to `TRUE` enables the Time Zone Offset feature.

SeparateCentury

- **Description:**

  Indicates whether Content Server supplies one or two lists to users for year inputs.

- **Syntax:**

  ```
  SeparateCentury=FALSE
  ```

- **Values:**

  `TRUE` or `FALSE`. The default value is `FALSE`.

  Setting this parameter to `TRUE` supplies two lists to users for year inputs: one list for the century, 19 and 20, and one list for the decade, 00 through 99. If you leave the default value, `FALSE`, one list for year inputs is supplied.

7.3.12 [dbconnection:connection_name]

The `[dbconnection:`*`<connection_name>`*`]` section defines database connection information and options. Each of the parameters in this section is set by the Administrator during the installation of Content Server. The values are managed through the Content Server Administration page.

For more information, see “Maintaining an Existing Database“ on page 297.

7.3.13 [DCS]

The settings in the `[DCS]` section control the behavior of the indexing function of the Document Conversion Service, DCS. The DCS uses different conversion filters to convert native data to HTML or raw text within an intermediate data flow process. After converting the documents, the DCS makes the data available to the Update Distributor process for indexing. For more information about conversion filters, see *OpenText Content Server - Administering Search (LLESWBS-AGD)*.

The `[DCS]` section of the `opentext.ini` file contains the following parameters:

- “LogFileSizeInMB” on page 108
- “LogMode” on page 109
- “logLevel” on page 109
- “maxcontentrefsize” on page 110
- “maxoctetsize” on page 110
- “maxuptime” on page 110
- “mod” on page 111
- “modreq” on page 111
- “NumThreads” on page 112
- “NumRollingLogFiles” on page 112
- “QueueSize” on page 113
- “rulesfile” on page 113
- “Securedelete” on page 113

Some of the parameters in the `[DCS]` section of the `opentext.ini` file are also in the `[FilterEngine]` section. The `[DCS]` parameters perform the same function as the corresponding `[FilterEngine]` parameters; however, setting the values for the parameters in the `[DCS]` section overrides the settings in the `[FilterEngine]` section. If no value is specified in the `[DCS]` section, the value is inherited from the `[FilterEngine]` section. This page contains information about the following parameters shared by the `[DCS]` and `[FilterEngine]` sections:

- “dllpath” on page 114
- “logfile” on page 114

LogFileSizeInMB

- **Description:**

  Specifies a limit, in MB, on the maximum size of a log file.
- **Syntax:**

  ```
  LogFileSizeInMB=100
  ```
- **Values:**

An integer greater than, or equal to, **1**. The default value is `100`.

logLevel

- **Description:**

  Specifies the events and information that should be written to the log file.

- **Syntax:**

  ```
  logLevel=1
  ```

- **Values:**

  Integer values `0`, `1`, `2`, `3`, or `4`. The default value is `1`.

  The following table contains descriptions of the valid values for the `logLevel` parameter.

Value	Description
0	Disables logging
1	Only errors and documents that could not be indexed are logged. This is the default value.
2	Logs everything from `logLevel=1`, and also logs DCS events. Examples of these events include loading a conversion filter and shutting down the conversion process.
3	Logs everything from `logLevel=2`, and also logs document conversion statistics and document information. This information includes the conversion time, size of the input file, document MIME type, OTURN, and which conversion filter was used to convert the document.
4	Logs everything from `logLevel=3`, and also logs iPool processing events, and log messages generated by the conversion filters. This level should only be used to help identify problems in the data flow.

LogMode

- **Description:**

  Specifies how the DCS processes are recorded in one or more log files.

- **Syntax:**

  ```
  LogMode = Rolling
  ```

- **Values:**

  Valid values are:

- `Rolling` – saves and closes the existing log file and creates a new file, which is the default.
- `Single` – adds any new information to the end of the current log file, which is the traditional logging mode. The parameters “LogFileSizeInMB” on page 108 and “NumRollingLogFiles” on page 112 are ignored.
- `Segmented` – rolls over to new files when an existing log file is full, as defined by the size specified in “LogFileSizeInMB” on page 108. The parameter “NumRollingLogFiles” on page 112 is ignored.

maxcontentrefsize

- **Description:**

  Specifies the maximum size, in kilobytes, of EFS (External File Storage) files the DCS can pre-load. This setting avoids multiple disk hits to the EFS, and in some situations, this can result in dramatic performance improvement. This setting has no effect on non-EFS files.

- **Syntax:**

  ```
  maxcontentrefsize=10240
  ```

- **Values:**

  An integer greater than, or equal to, zero. The default value is `10240`. A value of zero disables this parameter.

maxoctetsize

- **Description:**

  Specifies the maximum size, in kilobytes, of program files that can be converted by the DCS. Some unusual text documents are occasionally identified as `application octet-stream` files. Rather than discard such a document, the DCS attempts to convert it to the UTF-8, or Unicode, character set. If this is successful, the document is indexed.

  Files larger than the specified size will be discarded without the UTF-8 conversion. Smaller values may prevent more text documents from being indexed. Larger values may increase the amount of bad tokens indexed by the search engine, which will impact search performance.

- **Syntax:**

  ```
  maxoctetsize=256
  ```

- **Values:**

  An integer. The default value is `256`.

maxuptime

- **Description:**

  Specifies the maximum time period, in minutes, before the DCS is restarted. When your Content Server is running normally, the DCS will exit without an error and the Admin Server will immediately restart a new instance. For a dataflow instance of the DCS, it is preferable to define "maxtransactions" on page 119 instead of the `maxuptime` parameter.

Important
Do not modify the value of this parameter unless directed to do so by OpenText Customer Support.

- **Syntax:**

  ```
  maxuptime=1440
  ```

- **Values:**

  An integer greater than, or equal to, zero. The default value is `0`, which is disabled.

mod

- **Description:**

  Specifies the section of the `opentext.ini` file that contains the configuration for a conversion filter. The `[DCS]` section may contain several `mod` parameters that correspond to different conversion filters.

> **Caution**
> Modifying the value of this parameter may prevent the DCS from functioning, or from functioning correctly. Do not modify the values of these parameters unless directed to do so by OpenText Customer Support.

- **Values:**

  The following table contains the default values for the `mod` parameter.

Name	Value
modx01	QDF
mod03	Summarizer
modx04	DCSxpdf
modx05	Languageid
modx06	DCSmail

Note: The character *x* specifies that the conversion filter process will be carried out within a worker process.

The Summarizer filter process should be carried out within the DCS, and not a worker process.

modreq

- **Description:**

Specifies the request handler used by the DCS. The request handler accepts input documents from a specific source type, such as an iPool, socket, or pipe, and delivers the documents to the DCS to perform the conversion. After the conversion is finished, the converted documents are returned to the request handler and delivered to their appropriate destination, such as a client or an iPool.

> **Caution**
> Modifying the value of this parameter may prevent the DCS from functioning, or from functioning correctly. Do not modify the value of this parameter unless directed to do so by OpenText Customer Support.

- **Values:**

  The default value is `DCSipool`.

modx10

- **Description:**

  This parameter is required in order to use the OpenText Document Filters with Content Server on the Linux® platform. For more information, see *OpenText Content Server - Administering Search (LLESWBS-AGD)*.

- **Syntax:**

  ```
  modx10=DCSIm
  ```

- **Values:**

  The only allowed value is `DCSIm`.

NumRollingLogFiles

- **Description:**

  Specifies the maximum number of DCS log files. After the number of log files you specify is created, the oldest is deleted.

- **Syntax:**

  ```
  NumRollingLogFiles=10
  ```

- **Values:**

  An integer greater than `0`. The default value is `10`.

NumThreads

- **Description:**

  Specifies the maximum number of concurrent document conversion operations that the DCS can perform. Changing the default value affects document conversion performance.

- **Syntax:**

```
NumThreads=2
```

- **Values:**

  An integer between `1` and `64`. The default value is `2`.

QueueSize

- **Description:**

  Specifies the maximum number of documents that the DCS queues when the maximum number of concurrent document conversions is reached.

  Important
  OpenText strongly recommends that you do not modify the value of this parameter.

- **Values:**

  An integer. The default value is `20`.

rulesfile

- **Description:**

  Specifies the file name that defines the rules for document conversion processing of various MIME types.

  Important
  OpenText strongly recommends that you do not modify the value of this parameter.

- **Values:**

  An absolute path. The default value is `<Content Server_home>\config\dcsrules.txt`, where <*Content Server_home*> is the root of your Content Server installation.

Securedelete

- **Description:**

  Specifies whether the temporary files generated by the DCS are scrubbed with secure delete patterns to make them non-recoverable.

  During index creation, the DCS generates temporary files that may contain text or other content extracted from the files being indexed. When a temporary file is no longer needed, the data flow uses normal system calls to delete it. In most cases, this removes the file entry but allows an image of the file to remain on disk.

  Security-conscious sites may want to set a *secure delete level*, which determines how the system overwrites the image left on the disk. The `Securedelete` parameter sets the secure delete level for the DCS.

  Note: If you set the `Securedelete` parameter to anything other than the default, OpenText recommends that you set the secure delete level for `iPools` to the same value. For more information about the secure delete level, see *OpenText Content Server - Administering Search (LLESWBS-AGD)*.

- **Syntax:**

  ```
  Securedelete=0
  ```

- **Values:**

  An integer between `0` and `4`, zero and four. By default, this parameter does not appear in the `opentext.ini` file, which is equivalent to `Securedelete=0`.

  Setting this parameter to `0` turns off the secure delete functionality for DCS. Setting this parameter to any larger value represents increasingly complex file scrubs.

dllpath

- **Description:**

  Specifies the location of the directory containing Content Server's conversion filters. A document created by a word processor, such as Microsoft Word, contains formatting information that is not necessary or required for searching. Conversion filters extract text content that is suitable for reading and indexing from word processor files.

- **Syntax:**

  ```
  dllpath=C:\OPENTEXT\filters
  ```

- **Values:**

  An absolute path. The default value is `<Content Server_home>\filters`, where <*Content Server_home*> is the root of your Content Server installation.

logfile

- **Description:**

  Specifies the location and prefix for the Document Conversion log file. The admin port number assigned to this process is appended to the log file, followed by the `.log` suffix. This prevents multiple processes from writing to the same file.

  Note: This is a required parameter. To disable logging, set “logLevel” on page 109=0.

- **Syntax:**

  ```
  logfile=C:\OPENTEXT\logs\dcs
  ```

- **Values:**

  An absolute path. The default value is `<Content Server_home>\logs\dcs`, where <*Content Server_home*> is the root of your Content Server installation.

7.3.14 [DCSIm]

The settings in the `[DCSIm]` section control the configuration of the OpenText Document Filters (IM Filter), that the Document Conversion Service (DCS) uses. The OpenText Document Filters is an installable set of Document Conversion Service components and associated files that extend the MIME type detection, text-extraction, and document-conversion capabilities of Content Server.

For more information about the IM Filter, see *OpenText Content Server - Administering Search (LLESWBS-AGD)*

The `[DCSIm]` section of the `opentext.ini` file contains information about the following parameters:

- "dllpath" on page 115
- "lib" on page 115
- "outputoleinfo" on page 115
- "viewpagerange" on page 116
- "WordExcel2010HtmlViewOn" on page 116
- "x-timeout" on page 116

dllpath

- **Description:**

  Specifies the path to the directory where the DCSIm filter resources are installed.

- **Syntax:**

  ```
  dllpath=<Content_Server_home>/filters/image
  ```

- **Values:**

  An absolute path. The default value is *`<Content_Server_home>`*`/filters/image`.

lib

- **Description:**

  Specifies the name of the library to be loaded by the DCS. A library is a list of operations associated with a conversion filter that the DCS reads to perform the conversion.

- **Syntax:**

  ```
  lib=DCSIm
  ```

- **Values:**

  The default value is `DCSIm`. Modifying the value of this parameter may prevent the DCS from functioning or functioning properly. Do not modify the value of this parameter unless directed to do so by OpenText Customer Support.

outputoleinfo

- **Description:**

Specifies whether DCSIm should extract OLE properties from the document and retrieve only the OLE metadata tags listed in the `metadataTags.txt` file. OLE is a program-integration technology that is supported by all Microsoft Office programs. OLE allows information to be shared among different programs.

If this parameter is enabled, DCSIm extracts the standard OLE properties as well as any custom OLE properties associated with a document.

Note: This setting applies to the Custom Regions in Office 2007 and 2010 documents such as Word, Excel, and PowerPoint.

- **Syntax:**

  `outputoleinfo=TRUE`

- **Values:**

  When `outputoleinfo=TRUE` only OLE metadata tags (listed in the `metadataTags.txt file`) are retrieved. When `outputoleinfo=FALSE`, or is not defined, then all metadata tags are retrieved.

viewpagerange

- **Description:**

  Specifies which pages of a document DCSIm will convert to HTML for View as Web Page.

- **Syntax:**

  `viewpagerange=all`

- **Values:**

  A range of integers from `1` to *X*, or `all`. For example, to convert only the first 10 pages to HTML, set `viewpagerange=1-10`. The default value is `all`.

WordExcel2010HtmlViewOn

- **Description:**

  Specifies whether View as Web Page for Office 2010 formats Word and Excel is enabled in DCSIm.

- **Syntax:**

  `WordExcel2010HtmlViewOn=TRUE`

- **Values:**

  `TRUE` or `FALSE`. When `WordExcel2010HtmlViewOn=FALSE`, or is not defined, View as Web Page for Office 2010 formats Word and Excel is not enabled.

x-timeout

- **Description:**

  Specifies the maximum number of seconds to wait before terminating a document conversion worker process. You configure this parameter when the default value specified in the timeout parameter is inappropriate. You configure the timeout parameter for each conversion filter. For example, some conversion filters convert documents slower than other conversion filters. In this case, the timeout default value of 30 seconds may not be applicable, as the average conversion time is longer than this value. In this case, you can modify the x-timeout value to a higher and more appropriate value.

Warning

OpenText strongly recommends that you do not modify the value of this parameter.

- **Syntax:**

  ```
  x-timeout=30
  ```

- **Values:**

  The default value is inherited from the `timeout` parameter of the `[DCSworker]` section of the opentext.ini file. The default value is `30` seconds.

Note: When both the `x-timeout` value and the `timeout` value in the "[DCSworker]" on page 127 section of the opentext.ini file are specified, the lower value takes effect first, and the document conversion worker process is terminated.

The x-timeout parameter is only functional when the conversion filter it modifies is managed by a worker process. For more information about configuring a worker process, see "[DCS]" on page 108.

7.3.15 [DCSipool]

The `[DCSipool]` section controls options specific to the configuration of data interchange pools, *IPools*, for the Document Conversion Service, DCS. The DCS converts documents from their native formats to HTML or raw text for viewing and indexing purposes. IPools are temporary storage areas that connect the processes in a data flow. As data passes through a data flow, it is deposited in IPools. The DCS reads data from IPools so that it can process data and convert it to HTML.

If the thumbnail generation feature is enabled, the DCS also generates thumbnail images for documents automatically.

This page contains information about the following parameters shared by the `[DCSipool]` and "[FilterEngine]" on page 134 sections:

• "lib" on page 118	• "MaxMetaSize" on page 118	• "maxrequests" on page 118

Some of the parameters in the `[DCSipool]` section of the `opentext.ini` file are also in the `[FilterEngine]` section. The `[DCSipool]` parameters perform the same function as the corresponding `[FilterEngine]` parameters; however, setting the values for the parameters in the `[DCSipool]` section overrides the settings in the `[FilterEngine]` section. If no value is specified in the `[DCSipool]` section, the value is inherited from the `[FilterEngine]` section.

The [DCSipool] section of the opentext.ini file contains information about the following parameters:

• "MaxFileSize" on page 119 • "minwindow" on page 120	• "maxtime" on page 119 • "maxtransactions" on page 119	• "ThumbnailLocation" on page 120 • "window" on page 120

lib

- **Description:**

  Specifies the name of the *library* to be loaded by the DCS. A library is a list of operations associated with a conversion filter that the DCS reads to perform conversion.

  Caution
  Modifying the value of this parameter will prevent DCS from initializing. Do not modify the value of this parameter.

- **Values:**

  The default value is `dcsipool`.

MaxMetaSize

- **Description:**

  Specifies the maximum size, in MB, of metadata that can be stored in memory while the corresponding document is being converted. If any metadata exceeds this value, it will be stored in a temporary file until the associated document has been converted.

  Important
  OpenText strongly recommends that you do not modify the value of this parameter.

- **Values:**

  An integer greater than one. The default value is `8`.

  Note: Specifying a value larger than the default may cause the DCS to consume more memory.

maxrequests

- **Description:**

  Specifies the number of documents that the DCS reads from the IPool.

  Important
  OpenText strongly recommends that you do not modify the value of this parameter.

- **Values:**

  The value should correspond to the `NumThreads` parameter in the [DCS] section of the `opentext.ini` reference section so that the indexing process can synchronize effectively. For further information, see "[DCS]" on page 108

  Note: This parameter is not set in the default `opentext.ini` file. When no value is specified, the default value matches the setting specified for the `NumThreads` parameter in the [DCS] section.

MaxFileSize

- **Description:**

  Specifies the maximum size, in MB, of a file that can be converted in memory.

- **Syntax:**

  ```
  MaxFileSize=8
  ```

- **Values:**

  An integer greater than one. The default value is `8`.

maxtime

- **Description:**

  Specifies the maximum amount of time, in milliseconds, to allow for processing of an IPool transaction. When a transaction exceeds this time limit, the transaction is committed after the current IPool message has been fully processed, regardless of whether the `window` or `minwindow` criteria have been satisfied.

  This parameter is the last of three throughput-limiting mechanisms in the `[FilterEngine]` section of the `opentext.ini` file, after the `window` and `minwindow` parameters.

- **Syntax:**

  ```
  maxtime=120000
  ```

- **Values:**

  An integer greater than, or equal to, one. The default value is `120000`, or two minutes.

maxtransactions

- **Description:**

  Specifies the maximum number of iPool messages to process before the DCS is restarted. When your Content Server is running normally, the DCS will exit without an error and the Admin Server will immediately restart a new instance. The "maxuptime" on page 110 parameter can also be used to restart the DCS, but OpenText recommends you use the `maxtransactions` parameter.

! **Important**
Do not modify the value of this parameter unless directed to do so by OpenText Customer Support.

- **Syntax:**

  ```
  maxtransactions=5000
  ```

- **Values:**

  An integer greater than, or equal to, zero. The default value is `0`, which is disabled.

minwindow

- **Description:**

  Specifies the minimum number of IPool messages to process from the read IPool area before the DCS commits an IPool transaction. If the number of available messages in the read area is less than the value specified for the `minwindow` parameter, the transaction will be committed after the DCS processes the last IPool message.

  This parameter is the second of three throughput-limiting mechanisms in the `[FilterEngine]` section of the `opentext.ini` file, after the `window` parameter and before the `maxtime` parameter.

- **Syntax:**

  ```
  minwindow=5
  ```

- **Values:**

  An integer greater than, or equal to, one. The default value is `5`.

ThumbnailLocation

- **Description:**

  Specifies the location of the temporary directory in which the DCS generates and stores thumbnail image files before transferring them to Content Server.

  This value must be the same on all Admin server instances in a cluster, in particular, on servers that run data flow Data Conversion processes and the Content Server agent that tests objects in the system volume.

- **Syntax:**

  ```
  ThumbnailLocation=C:\OPENTEXT\tmp
  ```

- **Values:**

  An absolute path. The default value is `<Content_Server_home>\tmp`, where *<Content_Server_home>* is the root of your Content Server installation.

window

- **Description:**

Specifies the maximum number of IPool messages to be processed from the IPool read area before the DCS commits an IPool transaction.

This parameter is the first of three throughput-limiting mechanisms in the `[FilterEngine]` section of the `opentext.ini` file, followed by the `minwindow` and `maxtime` parameters.

- **Syntax:**

  ```
  window=10
  ```

- **Values:**

  An integer greater than, or equal to, one. The default value is `10`.

  Note: Setting this value higher than the default improves conversion filter throughput but also increases the amount of disk space used by the DCS.

7.3.16 [DCSpipe]

The settings in the `[DCSpipe]` section control the inter-process communication between a Document Conversion Service, DCS, client process and the DCS. The DCS converts documents from their native formats to HTML or raw text for viewing and indexing purposes. DCSs are managed by Admin servers. The parameters in the `[DCSpipe]` section are only used when the Admin server that manages a DCS is not running, or the DCS is disabled. In these cases, a new DCS service that reads from the parameters specified in the `[DCSpipe]` section of the `opentext.ini` file is launched.

Lib

- **Description:**

  Specifies the name of the *library* to be loaded by the DCS. A library is a list of operations associated with a conversion filter that the DCS reads to perform conversion.

  Modifying the value of this parameter may prevent the DCS from functioning or from functioning properly.

  Important
  Do not modify the value of this parameter unless directed to do so by OpenText Customer Support.

- **Values:**

  The default value is `dcspipe`.

7.3.17 [DCSservers]

The `[DCSservers]` section is a compilation of running Document Conversion Service (DCS) servers in Content Server. The DCS converts documents from their native formats to HTML or raw text for viewing and indexing purposes. DCSs are managed by Admin servers. Clients of DCS, such as LLView and hit highlight, use this section to discover available DCS servers. This list is refreshed each time Content Server is required to load an Admin server.

Server1

- **Description:**

  Specifies an enumeration of available DCS servers.

  The value of this parameter is set automatically and updated periodically by the Admin server.

  Important
  Do not modify the value of this parameter unless directed to do so by OpenText Customer Support.

- **Values:**

  An integer. The value of this parameter is generated dynamically.

SpawnExe

- **Description:**

  Specifies the name of the DCS binary that Content Server uses to perform document conversion operations. The value of this parameter is set automatically and updated periodically by the Admin server.

  Important
  Do not modify the value of this parameter unless directed to do so by OpenText Customer Support.

- **Values:**

  The default value is `dcs.exe` on Windows. On other platforms, the default setting is `dcs`.

SpawnIni

- **Description:**

  Specifies the ini file to be used when DCS is not persistent. The value of this parameter is set automatically and updated periodically by the Admin server.

  Important
  Do not modify the value of this parameter unless directed to do so by OpenText Customer Support.

- **Values:**

An absolute path. The default value is *<Content_Server_home>*/config/opentext.ini, where <*Content_Server_home*> is the root of your Content Server installation.

7.3.18 [DCSview]

The settings in the [DCSview] section control the operation of the Document Conversion Service, DCS, for viewing and hit highlighting documents inside Content Server. The DCS converts documents from their native formats to HTML or raw text. DCSs are managed by the Admin servers. The parameters in the [DCSview] section are only used when the Admin server is not running or the DCS managed by the Admin server is not enabled. You can also configure this service when you configure an Admin server. The parameters you specify when you configure an Admin server override the values in the [DCSview] section of the opentext.ini file. For more information about the parameters you can configure when you configure an Admin server, see "Configuring Server Parameters and Settings" on page 73.

The [DCSview] section of the opentext.ini file contains information about the following parameters:

• "logLevel" on page 123 • "mod" on page 124	• "modreq" on page 125 • "NumThreads" on page 125	• "QueueSize" on page 126 • "rulesfile" on page 126

Some of the parameters in the [DCSview] section of the opentext.ini file are also in the [FilterEngine] section. The [DCSview] parameters perform the same function as the corresponding [FilterEngine] parameters; however, setting the values for the parameters in the [DCSview] section overrides the settings in the [FilterEngine] section. If no value is specified in the [DCSview] section, the value is inherited from the [FilterEngine] section.

This page contains information about the following parameters shared by the [DCSview] and [FilterEngine] sections:

• "dllpath" on page 126	• "logfile" on page 126	

logLevel

- **Description:**

  Specifies the events and information that should be written to the log file.

- **Syntax:**

  logLevel=1

- **Values:**

  Integer values 0, 1, 2, 3, or 4. The default value is 1.

  The following table contains descriptions of the valid values for the logLevel parameter.

Value	Description
0	Disables logging
1	Only errors and documents that could not be indexed are logged. This is the default value.
2	Logs everything from `logLevel=1`, and also logs DCS events. Examples of these events include loading a conversion filter and shutting down the conversion process.
3	Logs everything from `logLevel=2`, and also logs document conversion statistics and document information. This information includes the conversion time, size of the input file, document MIME type, OTURN, and which conversion filter was used to convert the document.
4	Logs everything from `logLevel=3`, and also logs iPool processing events, and log messages generated by the conversion filters. This level should only be used to help identify problems in the data flow.

mod

- **Description:**

  Specifies the section of the `opentext.ini` file that contains the configuration for a conversion filter. The `[DCSview]` section may contain several `mod` parameters that correspond to different conversion filters.

  Caution

  Modifying the value of this parameter may prevent the DCS from functioning, or from functioning properly. Do not modify the values of these parameters unless directed to do so by OpenText Customer Support.

- **Values:**

  The following table contains default values for the `mod` parameter.

Name	Value
modx02	QDF
modx03	DCStext
modx04	DCSxpdf
modx06	DCSmail

Note: The character *x* specifies that the conversion filter process will be carried out within a worker process.

modreq

- **Description:**

  Specifies the request handler used by the DCS. The request handler accepts input documents from a specific source type, such as an IPool, socket, or pipe, and delivers the documents to the DCS to perform the conversion. After the conversion is finished, the converted documents are returned to the request handler and delivered to their appropriate destination, such as a client or an IPool.

  Caution
  Modifying the value of this parameter may prevent the DCS from functioning, or from functioning properly. Do not modify the value of this parameter unless directed to do so by OpenText Customer Support.

- **Values:**

  The default value is `DCSpipe`.

modx10

- **Description:**

  This parameter is required in order to use the OTDF Filter with Content Server on the Linux® platform.

- **Syntax:**

  ```
  modx10=DCSIm
  ```

- **Values:**

  The only allowed value is `DCSIm`.

NumThreads

- **Description:**

  Specifies the maximum number of concurrent document conversion operations that the DCS can perform. Changing the default value affects document conversion performance.

- **Syntax:**

  ```
  NumThreads=1
  ```

- **Values:**

  An integer between `1` and `64`. The default value is `1`.

QueueSize

- **Description:**

  Specifies the maximum number of documents that the DCS queues when the maximum number of concurrent document conversions is reached.

  Important
  OpenText strongly recommends that you do not modify the value of this parameter.

- **Values:**

  An integer. The default value is `50`.

rulesfile

- **Description:**

  Specifies the file name that defines the rules for document conversion processing of various MIME types.

  Important
  OpenText strongly recommends that you do not modify the value of this parameter.

- **Values:**

  An absolute path. The default value is `<Content_Server_home>\config\dcsrest.txt`, where *<Content_Server_home>* is the root of your Content Server installation.

dllpath

- **Description:**

  Specifies the location of the directory containing Content Server's conversion filters. A document created by a word processor, such as Microsoft Word, contains formatting information that is not necessary or required for searching. Conversion filters extract text content that is suitable for reading and indexing from word processor files.

- **Syntax:**

  ```
  dllpath=C:\OPENTEXT\filters
  ```

- **Values:**

  An absolute path. The default value is `<Content_Server_home>\filters`, where *<Content_Server_home>* is the root of your Content Server installation.

logfile

- **Description:**

Specifies the location and prefix for the Document Conversion log file. The admin port number assigned to this process is appended to the log file, followed by the .log suffix. This prevents multiple processes from writing to the same file.

- **Syntax:**

  ```
  logfile=C:\OPENTEXT\logs\dcsview
  ```

- **Values:**

  An absolute path. The default value is `<Content_Server_home>\logs\dcsview`, where <*Content_Server_home*> is the root of your Content Server installation.

  Note: This is a required parameter. To disable logging, set “logLevel” on page 123 to `0`.

7.3.19 [DCSworker]

The settings in the `[DCSworker]` section control the behavior of the worker processes managed by the Document Conversion Service (DCS). The DCS converts documents from their native formats to HTML or raw text for viewing and indexing purposes. The DCS sends documents to a worker process named `dcsworker.exe`. This worker process delegates conversion operations to the appropriate conversion filters after receiving requests from the DCS. It loads the requested conversion filter and performs the conversion in an isolated environment. This prevents damaging processes from terminating the DCS.

The `[DCSworker]` section of the `opentext.ini` file contains information about the following parameters:

- “fastinit” on page 127
- “lib” on page 128
- “maxcalls” on page 128
- “timeout” on page 128
- “workerexe” on page 129
- “x-maxmemory” on page 129

fastinit

- **Description:**

  Specifies whether external conversion filters should be loaded when the DCS starts.

- **Syntax:**

  ```
  fastinit=FALSE
  ```

- **Values:**

  `TRUE` or `FALSE`. The default setting is `FALSE`.

  Setting this parameter to `TRUE` instructs the DCS to wait until the conversion filter is required for the conversion process before loading it. Setting this parameter to `TRUE` results in a quicker performance time.

lib

- **Description:**

  Specifies the name of the *library* to be loaded by the DCS. A library is a list of operations associated with a conversion filter that the DCS reads to perform conversion.

  > **Caution**
  > Modifying the value of this parameter may prevent the DCS from functioning, or from functioning properly. Do not modify the value of this parameter unless directed to do so by OpenText Customer Support.

- **Values:**

  The default value is `dcsworker`.

maxcalls

- **Description:**

  Specifies the maximum number of conversion operations that a worker process should perform before it is stopped. A worker process will stop once its document conversion quota reaches the value specified in the `maxcalls` parameter. This mechanism is provided to prevent conversion filters that may have memory leaks from using too much memory.

- **Syntax:**

  `maxcalls=200`

- **Values:**

  The default value is `200`.

  Note: This setting can be customized for each conversion filter by configuring the `x-maxcalls` parameter in the `opentext.ini` file section for the appropriate conversion filter.

timeout

- **Description:**

  Specifies the maximum number of seconds to wait before terminating a document conversion worker process.

  The DCS monitors the time that worker processes spend converting documents and terminates the worker processes that exceed this limit. This timeout threshold is defined by the `timeout` parameter.

  When the worker process tries to convert a corrupt or otherwise badly formed document, it fails and returns an error code to the worker process. Some documents, however, can cause the filtering system to remain in an infinite processing loop. On rare occasions, the conversion filter progressively uses up system resources while in this infinite loop.

The worker process has a default `timeout` value of 30 seconds, after which it stops the worker process. However, if the worker process is using up memory quickly, it could consume all the available memory before the 30 seconds have elapsed. In this case, you can lower the `timeout` value so that the conversion filter will not consume all the memory before it times out.

The value of the `timeout` parameter should be as low as possible, without causing the conversion process to end before a valid document can be converted. You can estimate an appropriate `timeout` value by enabling logging for a reasonable period of time, for example 24 hours, and examining the maximum amount of time the process spends converting a valid document. The length of the maximum valid conversion time is usually a small number of seconds. Once you have determined this value, you can change the `timeout` value to one and a half or two times the maximum valid conversion time. The additional time allows for documents that are larger than those that were converted during the test period.

- **Syntax:**

  ```
  timeout=30
  ```

- **Values:**

  An integer greater than, or equal to, one. The default value is `30`.

> **Note:** This parameter also appears in the `[FilterEngine]` section of the `opentext.ini` file. This parameter performs the same function as the corresponding `[FilterEngine]` parameter; however, setting the value for this parameter in the `[DCSworker]` section overrides the setting in the `[FilterEngine]` section. If no value is specified in the `[DCSworker]` section, the value is inherited from the `[FilterEngine]` section.
>
> This setting can be customized for each conversion filter by configuring the `x-timeout` parameter in the `opentext.ini` file section for the appropriate conversion filter.

workerexe

- **Description:**

  Specifies the name of the worker process program used by Content Server to perform document conversion operations.

> **Important**
>
> OpenText strongly recommends that you do not modify the value of this parameter.

- **Values:**

  The default value is `dcsworker.exe` on Windows. On other platforms, the default value is `dcsworker`.

x-maxmemory

- **Description:**

Specifies the maximum memory, in MB, that a worker process will use to perform document conversion operations.

- **Syntax:**

  ```
  x-maxmemory=2048
  ```

- **Values:**

  An integer greater than, or equal to, `128`. Using a lower value is possible, but this will cause the worker process to end before the filters are even loaded into memory. The default value is `2048` (2GB). Setting to `0` will disable the memory limit.

7.3.20 [DCSxpdf]

The `[DCSxpdf]` section controls the settings of the XPDF filter. The XPDF filter is used by the Document Conversion Service, DCS, to convert PDF files into plain text for indexing purposes.

The `[DCSxpdf]` section of the `opentext.ini` file contains information about the following parameters:

- "dllpath" on page 130
- "lib" on page 130
- "startdir" on page 131
- "x-maxcalls" on page 131
- "x-timeout" on page 131

dllpath

- **Description:**

  Specifies the path to the directory where the XPDF filter resources are installed.

- **Syntax:**

  ```
  dllpath=C:\OPENTEXT\filters\xpdf
  ```

- **Values:**

  An absolute path. The default value is `<Content_Server_home>\filters\xpdf`, where <*Content_Server_home*> is the root of your Content Server installation.

lib

- **Description:**

  Specifies the name of the *library* to be loaded by the DCS. A library is a list of operations associated with a conversion filter that the DCS reads to perform the conversion.

> **Caution**
> Modifying the value of this parameter may prevent the DCS from functioning, or from functioning properly. Do not modify the value of this parameter unless directed to do so by OpenText Customer Support.

- **Values:**

  The default value is `dcsxpdf`.

startdir

- **Description:**

  Specifies the path to the directory from which the XPDF filter executes.

- **Syntax:**

  ```
  startdir=C:\OPENTEXT\filters\xpdf
  ```

- **Values:**

  An absolute path. The default value is `<Content_Server_home>\filters\xpdf`, where <*Content_Server_home*> is the root of your Content Server installation.

x-maxcalls

- **Description:**

  Specifies the number of times a worker process is reused for processing documents. During document conversion, the DCS loads a worker process. The worker process loads the appropriate conversion filter and uses it to convert the document. To increase performance, the DCS reuses the worker process for multiple conversions. If the worker process encounters an error, the process is stopped before reaching the value specified in the `opentext.ini` file.

  Important
  OpenText strongly recommends that you do not modify the value of this parameter.

- **Values:**

  The default value is inherited from the `maxcalls` parameter of the `[DCSworker]` section of the `opentext.ini` file.

  Note: The `x-maxcalls` parameter is only functional when the conversion filter it modifies is managed by a worker process. For more information about configuring a worker process, see "[DCS]" on page 108.

  Specifying a value for `x-maxcalls` will override the value of `maxcalls` in the `[DCSworker]` section of the `opentext.ini` file.

x-timeout

- **Description:**

  Specifies the maximum number of seconds to wait before terminating a document conversion worker process. You configure this parameter when the default value specified in the `timeout` parameter is inappropriate. You configure the `timeout` parameter for each conversion filter. For example, some conversion filters convert documents slower than other conversion filters. In this case, the `timeout` default value of 30 seconds may not be applicable, as the average conversion time is longer than this value. In this case, you can modify the `x-timeout` value to a higher and more appropriate value.

Important
OpenText strongly recommends that you do not modify the value of this parameter.

- **Values:**

  The default value is inherited from the `timeout` parameter of the `[DCSworker]` section of the `opentext.ini` file.

  Note: The `x-timeout` parameter is only functional when the conversion filter it modifies is managed by a worker process. For more information about configuring a worker process, see "[DCS]" on page 108.

  Specifying a value for `x-timeout` will override the value of `timeout` in the `[DCSworker]` section of the `opentext.ini` file.

7.3.21 [EditableMimeTypes]

- **Description:**

  The `[EditableMimeTypes]` section is a list of MIME types that can be edited in Content Server using the Text Edit feature. For more information about the Text Edit feature, see *OpenText Content Server - Documents and Text Documents (LLESWBD-UGD)*.

- **Values:**

  The following is an example of the `[EditableMimeTypes]` section in the `opentext.ini` file:

```
[EditableMimeTypes]
text/html=TRUE
text/plain=TRUE
text/tab-separated-values=TRUE
text/xml=TRUE
text/xsl=TRUE
text/x-setext=TRUE
text/x-sgml=TRUE
```

7.3.22 [ExcludedMimeTypes]

- **Description:**

  The `[ExcludedMimeTypes]` section controls the behavior of the Enterprise Extractor process. By including a MIME type in this section, you instruct the Enterprise Extractor to ignore the *content* of documents of that MIME type, extracting only the *metadata* from documents of that MIME type in the Content Server database. Examples of metadata include the name of the document and the date the document was created.

  There are many file types whose content you may not want to index, such as audio and image files, whose content is not textual. When the content of such file types passes through the Enterprise Index data flow, it takes time and resources to process, even though it yields no useful result. Therefore, adding the MIME types of these and similar file types to the `[ExcludedMimeTypes]` section improves the efficiency of the Enterprise Index data flow by preventing data that you do not want to index from passing through it.

  Note: When a user adds a document to the Content Server database, Content Server records the MIME type that is reported by the user's web browser. Make certain that all web browsers used to connect to Content Server are configured properly. If a user's web browser is misconfigured, it may in some cases report an incorrect MIME type. If a web browser incorrectly reports a MIME type that appears in the `[ExcludedMimeTypes]` section, the content of the document is not extracted and indexed, even though its actual MIME type may be one for which you want to index content.

- **Values:**

  The following is an example of the `[ExcludedMimeTypes]` section in the `opentext.ini` file:

```
[ExcludedMimeTypes]
audio/basic=TRUE
audio/mpeg=TRUE
audio/x-aiff=TRUE
audio/x-wav=TRUE
image/gif=TRUE
image/ief=TRUE
image/jpeg=TRUE
image/tiff=TRUE
image/x-bmp=TRUE
image/x-cmu-raster=TRUE
image/x-pcx=TRUE
image/x-pic=TRUE
image/x-pict=TRUE
image/x-portable-anymap=TRUE
image/x-portable-graymap=TRUE
image/x-portable-pixmap=TRUE
image/x-rgb=TRUE
```

```
image/x-xbitmap=TRUE
image/x-xpixmap=TRUE
image/x-xwindowdump=TRUE
video/mpeg=TRUE
video/quicktime=TRUE
video/x-msvideo=TRUE
video/x-sgi-movie=TRUE
```

Note: Although the entries in the [ExcludedMimeTypes] section appear in the form *<MIME_type>*=TRUE, Content Server *ignores the value after the equals sign*. Setting a MIME type to FALSE has no effect. To include a particular MIME type for indexing, place a pound sign, #, in front of the MIME type entry or remove it altogether.

For more information about the Enterprise Extractor process and the Enterprise Index, see *OpenText Content Server - Administering Search (LLESWBS-AGD)* and *OpenText Content Server - Administering Search (LLESWBS-AGD)*.

7.3.23 [FetchMimeTypes]

- **Description:**

  The [FetchMimeTypes] section includes MIME types of files that Content Server should always download rather than attempt to open or fetch.

  Important
  OpenText recommends that you do not change any of the options in this section.

- **Values:**

  The following is an example of the [FetchMimeTypes] section in the opentext.ini file:

  ```
  [FetchMimeTypes]
  type1=application/x-msdownload
  type2=application/octet-stream
  ```

7.3.24 [FilterEngine]

The settings in the [FilterEngine] section control the central behavior of the Document Conversion Service, DCS. The DCS converts documents from their native formats to HTML or raw text for viewing and indexing purposes. To do so, the DCS uses document conversion filters. For information about document conversion filters, see *OpenText Content Server - Administering Search (LLESWBS-AGD)*.

There are three ways to configure the DCS.

- You can globally configure all DCSs at your site by setting the parameters in the [FilterEngine] section of the opentext.ini file.

- You can globally configure the specific settings for a conversion filter in one of the following `opentext.ini` file sections: `[DCS]`, `[DCSworker]`, `[DCSxpdf]`, `[DCSservers]`, `[DCSview]`, `[DCSpipe]`, `[DCSipool]`, `[QDF]`, `[DCSIm]`, and `[Summarizer]`.
- You can locally configure an individual DCS by setting command line arguments for the DCS.

Some of the parameters in the DCS sections of the `opentext.ini` file and some of the DCS command line arguments are also parameters in the `[FilterEngine]` section. The DCS parameters and command line arguments perform the same function as the corresponding `[FilterEngine]` parameters; however, setting the values for parameters in the DCS sections of the `opentext.ini` file or in the DCS command line arguments overrides the settings in the `[FilterEngine]` section.

The `[FilterEngine]` section of the `opentext.ini` file contains the following parameters:

- "conntenttruncsize" on page 135
- "dllpath" on page 135
- "encoding<n>" on page 136
- "logfile" on page 136
- "maxfilesize" on page 137
- "summary" on page 137
- "summaryhotwords" on page 137
- "summarysentences" on page 138
- "timeout" on page 138
- "tmpdir" on page 139
- "window" on page 139
- "minwindow" on page 140
- "maxtime" on page 140

conntenttruncsize

- **Description:**

  Specifies the maximum truncated size, in MB, DCS will use when converting documents from their native formats. When the document exceeds this limit, it will be truncated.

- **Syntax:**

  ```
  conntenttruncsize=8
  ```

- **Values:**

  An integer equal to or greater than `1`. The default value is `10`.

dllpath

- **Description:**

  Specifies the location of the directory containing Content Server's conversion filters. A document created by a word processor, such as Microsoft Word, contains formatting information that is not necessary or required for searching. Conversion filters extract text content that is suitable for reading and indexing from word processor files.

- **Syntax:**

```
dllpath=C:\OPENTEXT\filters
```

- **Values:**

  An absolute path. The default value is `<Content_Server_home>\filters`, where <*Content_Server_home*> is the root of your Content Server installation.

encoding<n>

- **Description:**

  The `encoding<n>` parameter allows you to specify multiple character encoding values, which can enable successful character encoding conversion for indexed documents. The DCS will attempt to detect the character encoding of text documents that are being indexed. If the DCS is not able to detect the encoding, it will attempt UTF-8 character encoding using the encoding values specified for this parameter. The DCS attempts to use the encoding values in the order that they are listed in the `[FilterEngine]` section. The DCS continues to attempt character encoding until it either is successful or runs out of valid encoding values to try. The first encoding value for which the data can be successfully converted is considered to be the correct encoding. Each `encoding<n>` entry in the `[FilterEngine]` section must have the following format: `encoding<n>=<encodingvalue>`, where *<n>* is a unique number.

  In the example shown in the *Syntax* section below, the DCS would attempt to convert documents using the `Shift JIS` encoding. If the `Shift JIS` encoding fails, the DCS would then attempt to use the `EUC-JP` encoding.

- **Syntax:**

  ```
  encoding1=Shift JIS
  encoding2=EUC-JP
  ```

- **Values:**

  A character encoding specification name. If no value is specified for this parameter, `ISO-8859-1` is used. If you do not include the `encoding<n>` parameter in the `opentext.ini` file at all, the DCS uses `Latin-1` encoding by default. For more information, contact OpenText Customer Support.

logfile

- **Description:**

  Specifies the location and prefix for the Document Conversion log file. The admin port number assigned to this process is appended to the log file, followed by the .log suffix. This prevents multiple processes from writing to the same file.

- **Syntax:**

  ```
  logfile=C:\OPENTEXT\logs\dcs
  ```

- **Values:**

  An absolute path. The default value is `<Content_Server_home>\logs\dcs`, where <*Content_Server_home*> is the root of your Content Server installation.

Note: This is a required parameter. To disable logging, set `logLevel` to `0`.

maxfilesize

- **Description:**

  Specifies the maximum size, in MB, of a file that can be converted in memory.

- **Syntax:**

  ```
  maxfilesize=8
  ```

- **Values:**

  An integer greater than one. The default value is `8`.

summary

- **Description:**

  Specifies whether the DCS generates summaries of the documents that it converts to HTML. If the user sets their search display options to show summaries, Content Server displays these summaries with search results on the Search Result page.

  By default, the `summary` parameter is set to `TRUE` on the command line of each DCS. To set the `summary` parameter to `FALSE`, you must modify the command line of each DCS rather than change the parameter in the `opentext.ini` file, since arguments set on the command line override the global parameters set in the `opentext.ini` file. For more information, see *OpenText Content Server - Administering Search (LLESWBS-AGD)*.

- **Values:**

  `TRUE` or `FALSE`. The default value is `TRUE`.

  A value of `TRUE` means that the DCS generates summaries. A value of `FALSE` means that the DCS does not generate summaries.

summaryhotwords

- **Description:**

  Specifies the number of hotwords that the summarizer uses to generate a document summary. Reducing this value may speed up summarization, but there are many other variables that also affect the speed of this process.

  > **Important**
  > OpenText strongly recommends that you not modify the value of this parameter.

- **Values:**

  An integer greater than, or equal to, one. The default value is `20`.

summarysentences

- **Description:**

  Specifies the number of sentences to generate in summaries.

- **Syntax:**

  ```
  summarysentences=5
  ```

- **Values:**

  An integer greater than, or equal to, one. By default, this parameter does not appear in the `[FilterEngine]` section of the `opentext.ini` file, which is equivalent to `summarysentences=5`.

timeout

- **Description:**

  Specifies the maximum number of seconds to wait before terminating a worker process.

  The DCS monitors the time that worker processes spend converting documents and terminates the worker processes that exceed this limit. This timeout threshold is defined by the `timeout` parameter.

  When the worker process tries to convert a corrupt or otherwise badly formed document, it fails and returns an error code to the DCS. Some documents, however, can cause the filtering system to remain in an infinite processing loop. On rare occasions, the conversion filter progressively uses up system resources while in this infinite loop.

  The DCS has a default `timeout` value of 30 seconds, after which it stops the worker process. However, if the worker process is using up memory quickly, it could consume all the available memory before the 30 seconds have elapsed. In this case, you can lower the `timeout` value so that the conversion filter will not consume all the memory before it times out.

  The value of the `timeout` parameter should be as low as possible, without causing the conversion process to end before a valid document can be converted. You can estimate an appropriate `timeout` value by enabling logging for a reasonable period of time, for 24 hours for example, and examining the maximum amount of time the process spends converting a valid document. The length of the maximum valid conversion time is usually a small number of seconds. Once you have determined this value, you can change the `timeout` value to one and a half or two times the maximum valid conversion time. The additional time allows for documents that are larger than those that were converted during the test period.

  The value of the `timeout` parameter can also be customized for each conversion filter. This is done by specifying the parameter `x-timeout` in the INI section of each conversion filter.

- **Syntax:**

  ```
  timeout=30
  ```

- **Values:**

  An integer greater than, or equal to, one. The default value is `30`.

tmpdir

- **Description:**

  Note: In the Windows version of Content Server, this value has no effect. All temporary files are written to the directory specified by the TMP environment variable.

  This parameter specifies the directory that DCSs use to store temporary conversion files. Temporary conversion files are files with `.in` and `.out` extensions, and the temporary files created by the filtering system. The value of this parameter can be no larger than 256 bytes.

  In Linux operating systems, OpenText recommends that you use the `/tmp` directory as the temporary directory for DCSs. Specifying a temporary file system, such as `/tmp` for Linux, significantly improves the performance of DCSs. In Linux versions of Content Server, the `tmpdir` parameter is set by default to `/tmp` during the installation of Content Server.

  Sometimes, temporary files are discarded by abnormally terminated worker processes in Linux. OpenText recommends that you clean up the temporary directory on a regular basis.

- **Syntax:**

  ```
  tmpdir=/tmp
  ```

- **Values:**

  An absolute path.

window

- **Description:**

  Specifies the maximum number of IPool messages to be processed from the IPool read area before the DCS commits an IPool transaction.

  This parameter is the first of three throughput-limiting mechanisms in the `[FilterEngine]` section of the `opentext.ini` file, followed by the `minwindow` and `maxtime` parameters.

- **Syntax:**

  ```
  window=10
  ```

- **Values:**

  An integer greater than, or equal to, one. The default value is `10`.

  Note: Setting this value higher than the default improves conversion filter throughput but also increases the amount of disk space used by the DCS.

minwindow

- **Description:**

  Specifies the minimum number of IPool messages to process from the read IPool area before the DCS commits an IPool transaction. If the number of available messages in the read area is less than the value specified for the `minwindow` parameter, the transaction will be committed after the DCS processes the last IPool message.

  This parameter is the second of three throughput-limiting mechanisms in the `[FilterEngine]` section of the `opentext.ini` file, after the `window` parameter and before the `maxtime` parameter.

- **Syntax:**

  ```
  minwindow=5
  ```

- **Values:**

  An integer greater than, or equal to, one. The default value is `5`.

maxtime

- **Description:**

  Specifies the maximum amount of time, in milliseconds, to allow for processing of an IPool transaction. When a transaction exceeds this time limit, the transaction is committed after the current IPool message has been fully processed, regardless of whether the `window` or `minwindow` criteria have been satisfied.

  This parameter is the last of three throughput-limiting mechanisms in the `[FilterEngine]` section of the `opentext.ini` file, after the `window` and `minwindow` parameters.

- **Syntax:**

  ```
  maxtime=120000
  ```

- **Values:**

  An integer greater than, or equal to, one. The default value is `120000`, or two minutes.

7.3.25 [filters]

The `[filters]` section controls the behavior of the document-viewing program, `llview`.

This page contains information about the following parameters:

• "autoRecMimeTypes" on page 141 • "filterPath" on page 141	• "logfile" on page 141 • "relativeLinkMimeTypes" on page 142	• "TypeSense" on page 142

autoRecMimeTypes

- **Description:**

  Instructs Content Server to perform autorecognition of files of the specified MIME types.

- **Syntax:**

  ```
  autoRecMimeTypes=application/octet-stream
  ```

- **Values:**

  A comma-separated list of valid MIME types. The default value is `application/octet-stream`.

filterPath

- **Description:**

  Location of the directory containing the document viewing filters.

- **Syntax:**

  ```
  filterPath=C:\OPENTEXT\filters\
  ```

- **Values:**

  An absolute path. The default value is `<Content_Server_home>\filters\`, where *<Content_Server_home>* is the root of your Content Server installation.

logfile

- **Description:**

  To instruct Content Server to log filter activity, add a `logfile` entry to the `[filters]` section. This activates filter logging and places the log entries in the file you specify.

- **Syntax:**

  ```
  logfile=C:\filters\<logfile_name>
  ```

- **Values:**

  An absolute path and file name. OpenText recommends:

<Content_Server_home>`\filters\`*<logfile_name>*, where *<Content_Server_home>* is the root of your Content Server installation and *<logfile_name>* is the name of your log file.

relativeLinkMimeTypes

- **Description:**

  When opening documents of a MIME type contained in this parameter, Content Server translates relative links within the document to other files so that clicking a relative link will fetch the proper item, provided the referenced item is also stored in Content Server.

- **Syntax:**

  ```
  relativeLinkMimeTypes=text/html,application/pdf
  ```

- **Values:**

  A comma-separated list of MIME types. The default value is: `relativeLinkMimeTypes=text/html,application/pdf`

TypeSense

- **Description:**

  Governs document view and fetch behavior.

- **Syntax:**

  ```
  TypeSense=BROWSER
  ```

- **Values:**

  `BROWSER` or `SERVER`. The default value is `BROWSER`.

  If this parameter is set to `BROWSER`, attempting to open a document causes Content Server to refer to the `ViewableMimeTypes` section. If the document's MIME type appears there, Content Server executes a fetch rather than attempting to open the document. If this parameter is set to `SERVER`, attempting to open a document causes Content Server to search the `INSOViewableMIMETypes` list in the `[filters]` section. If the document's MIME type appears there, Content Server opens the document rather than executing a fetch.

7.3.26 [general]

Many of the parameters in the `[general]` section are set during the installation process.

OpenText recommends that you use the Content Server Administration page to make changes to *INI* parameters. You should only modify the `opentext.ini` file when a parameter is not available on the Content Server Administration page. The following Content Server Administration pages describe changes you can make to the `[general]` section:

- “Understanding the Administration Page” on page 9

- “Configuring Basic Server Parameters” on page 73
- *OpenText Content Server - Notifications Administration (LLESWBN-AGD)*

This page contains information about the following parameters:

- “AdminIndexStyle” on page 143
- “AdminMailAddress” on page 144
- “adminpwd” on page 144
- “dbconnretries” on page 145
- “Debug” on page 145
- “DefaultContentRH” on page 146
- “DefaultRH” on page 147
- “DFTAutoLoginStr” on page 147
- “dftConnection” on page 147
- “DisableSelectReservedBy” on page 148
- “DisplayServerName” on page 148
- “DocModTimeInDays” on page 149
- “DocNewTimeInDays” on page 149
- “EnableAutoRestarts” on page 150
- “ExplorerServerName” on page 150
- “HaveSeenLicenseSetupPage” on page 150
- “HaveSeenModuleInstallPage” on page 151
- “HaveSeenSetupPage” on page 151
- “HaveValidatedDBAdminServers” on page 151
- “HaveValidatedEnterpriseDataSource” on page 152
- “HaveValidatedFacetsVolume” on page 152
- “HaveValidatedReSyncPage” on page 152
- “HaveValidatedSearchComponents” on page 153
- “HaveValidatedWarehouseVolume” on page 153
- “HTMLCharset” on page 154
- “htmlImagePrefix” on page 154
- “InstallAdminPort” on page 154
- “integrity” on page 155
- “LLIndexHTMLFile” on page 155
- “LLIndexRequiresLogin” on page 155
- “LogConfigPath” on page 155
- “Logpath” on page 156
- “MacBinaryDefault” on page 156
- “MailtoAddressSeparator” on page 156
- “MaxListingOnGroupExpn” on page 157
- “MaxUsersToListPerPage” on page 157
- “MessageClearInterval” on page 157
- “NavigationOption” on page 158
- “NewsDftExpiration” on page 158
- “NTPATH” on page 158
- “NTSERVICENAME” on page 159
- “NumOldLogs” on page 159
- “OTHOME” on page 160
- “PauseSleep” on page 160
- “Port” on page 160
- “Profile” on page 160
- “ProfileFormat” on page 161
- “ScheduleHandlerClearInterval” on page 162
- “Server” on page 162
- “UploadDirectory” on page 162
- “version” on page 163

AdminIndexStyle

- **Description:**

  Determines if the Content Server Administration page displays all sections and links at once, or if it displays the sections as tabs, with only the links under the selected tab displaying.

OpenText recommends that you modify this value using the Content Server Administration page, rather than edit the `opentext.ini` file directly. For more information, see "Understanding the Administration Page" on page 9.

- **Syntax:**

  ```
  AdminIndexStyle=all
  ```

- **Values:**

  Valid values are `all` or `tabs`. The default value is `all`.

Value	Description
`all`	Displays all sections and links at once. This is the default value, and corresponds to clicking "Show All Sections" on the Content Server Administration page.
`tabs`	Displays sections as tabs. Only the links in the selected tab display. This corresponds to clicking "Show As Tabs" on the Content Server Administration page.

AdminMailAddress

- **Description:**

  E-mail address of the Administrator. If you provide an e-mail address here, a link to e-mail the Administrator is created on the User Log-in page.

  OpenText recommends that you modify this value using the **Configure Server Parameters** page, rather than edit the `opentext.ini` file directly. For more information, see "Administrator E-mail Address" in "Configuring Basic Server Parameters" on page 73.

- **Syntax:**

  ```
  AdminMailAddress=<user_name>@<domain_name>.com
  ```

- **Values:**

  A valid e-mail address. The default value is null, `AdminMailAddress=`, which means no administrator email address is specified.

adminpwd

- **Description:**

  Encoded Content Server Administrator password.

  OpenText recommends that you modify this value using the **Configure Server Parameters** page, rather than edit the `opentext.ini` file directly. For more information, see "Content Server Administrator Password" in "Configuring Basic Server Parameters" on page 73.

- **Syntax:**

  ```
  adminpwd=<encoded_admin_password>
  ```

- **Values:**

An alphanumeric string. This parameter does not have a default value and is not displayed in the `opentext.ini` file until you enter a value in the **Content Server Administrator Password** field.

dbconnretries

- **Description:**

  Sets the number of times that Content Server tries to reconnect to the database if the database connection is lost. By default, this setting does not appear in the `opentext.ini` file, and its value defaults to `dbconnretries=15`.

  Content Server waits 1 millisecond between the first and second attempt to reconnect to the database. It then doubles the waiting period for each subsequent connection attempt (to 2 ms, then 4 ms, and so on).

  Tip: OpenText recommends that you do not set this value much higher than 15. If the value is set to 15, Content Server spends a little over a minute attempting to reconnect to the database. If the value is twenty, the total time spent is over fifteen minutes.

- **Syntax:**

  ```
  dbconnretries=15
  ```

- **Values:**

  A positive integer. The default value is 15.

Debug

- **Description:**

  Controls the level of debugging in Content Server. For more information, see *OpenText Content Server - Administering Search (LLESWBS-AGD)*.

  Logging adversely affects server performance. You should only enable logging for as long as is necessary to gather information on a particular problem.

  OpenText recommends that you modify this value using the **Configure Server Parameters** page, rather than edit the `opentext.ini` file directly. For more information, see “Server Logging Options” in “Configuring Basic Server Parameters” on page 73.

- **Syntax:**

  ```
  Debug=0
  ```

- **Values:**

  Valid values are `0`, `1`, `2`, and `11`. The default value is `0`, zero.

Value	Description
0	No logging. This is the default value.

Value	Description
1	Performs minimal server logging. Produces server thread and other log files in the *<Content_Server_home>*/logs directory. Log files produced include: • llserver.out • sockserv1.out • thread*<n>*.out (one per thread)
2	Performs all logging from Debug=1, as well as more detailed thread request logging, including information about the relevant environment variables in the thread logs.
11	Performs all logging from Debug=2, as well as enabling logging for CGI client process and Index Update engine, the Enterprise Extractor. Log files produced include: • llclient*<nnn>*.out (one per request to the CGI program from an end-user web browser) • llindexupdate*<nnn>*.out (one per start of the Enterprise Extractor) • indexupdateOut*<nnn>*.out (one per stop of the Enterprise Extractor) • receiver*<n>*.out (one each per thread)

Note: When using LLServlet instead of the Content Server CGI, llclient*<nnn>*.out is replaced by servletclient*<nnn>*.out. One file is generated for each thread number, as determined by your servlet container's Java Virtual Machine. Each time a client browser sends an LLservlet a request, a new servletclient*<nnn>*.out file is created. If a file name with that number *<nnn>* already exists, the request's information is appended to the end of the existing file.

DefaultContentRH

- **Description:**

  Sets the default content request handler. If the frames view of Content Server is displayed when users log in, when “DefaultRH” on page 147 is set to LL.FrameHome, this parameter controls which Content Server page is displayed in the right frame. If the no-frames view of Content Server is displayed when users log in, this parameter controls which Content Server page is displayed in the web browser window.

  OpenText recommends that you modify this value using the **Configure Server Parameters** page, rather than edit the opentext.ini file directly. For more information, see “Default User Start Page” in “Configuring Basic Server Parameters” on page 73.

- **Syntax:**

  ```
  DefaultContentRH=Enterprise.Home
  ```

- **Values:**

  The name of a valid request handler is required. Valid values are: Enterprise.Home, Personal.Home, and LL.Index. The default value is Enterprise.Home.

Value	Description
`Enterprise.Home`	This is the default value. It indicates that the **Enterprise Workspace** page is displayed when the user logs in.
`Personal.Home`	Indicates that the user's **Personal Workspace** page is displayed when the user logs in.
`LL.Index`	Indicates that the **About Content Server** page is displayed when the user logs in.

DefaultRH

- **Description:**

  Sets the default request handler. This parameter controls which view of Content Server is displayed when users log in using their web browsers.

- **Syntax:**

  `DefaultRH=Enterprise.Home`

- **Values:**

  The name of a valid request handler is required. Valid values are: `Enterprise.Home`, `Personal.Home`, `LL.Index`, and `LL.FrameHome`. The default value is `Enterprise.Home`.

  This value can only be set in the `opentext.ini` file.

Value	Description
`Enterprise.Home`	This is the default value. It indicates that the **Enterprise Workspace** page is displayed in a no-frames view of Content Server when users log in.
`Personal.Home`	Indicates that the user's **Personal Workspace** page is displayed in a no-frames view of Content Server when users log in.
`LL.Index`	Indicates that the **About Content Server** page is displayed in a no-frames view of Content Server when users log in.
`LL.FrameHome`	Indicates that the frames view of Content Server is displayed when users log in. When `DefaultRH` is set to `LL.FrameHome`, the Menubar is displayed in the left frame and the content of the right frame is controlled by “DefaultContentRH” on page 146.

DFTAutoLoginStr

- **Description:**

  This is OpenText proprietary information.

dftConnection

- **Description:**

  Default database connection.

- **Syntax:**

  `dftConnection=<default_database_connection>`

- **Values:**

  This parameter does not have a default value and is not displayed in the `opentext.ini` file until you enter a value. You set this value when you install Content Server and configure its database.

  The value must match the connection specified in the "[dbconnection:connection_name]" on page 108 section title. If there are multiple `dbconnection` sections, specify the connection that you want to use.

DisableSelectReservedBy

- **Description:**

  In Content Server, users can reserve a document to a group. The `DisableSelectReservedBy` parameter allows one group member to reserve a document, but have other members of the group work on it, and subsequently have a different member of the group check the document back in. The intended behavior is for Content Server to display a page that prompts the user to specify the user or group to which to reserve the document at the same time that the document is being downloaded to the web browser.

  If the user's web browser is configured to open the document's MIME type, the document is displayed directly in the web browser window and the user does not have the opportunity to specify the user or group to which they want to reserve the document. In particular, this problem has been reported with HTML documents in Microsoft Internet Explorer browsers. The user is thus unable to reserve documents of this MIME type using the Check-out method.

  Users experiencing this problem have two options:

  1. Reserve and then Fetch the document, rather than using Check-out.
  2. Add `DisableSelectReservedBy=TRUE` to the `[general]` section of the `opentext.ini` file. This disables the group check-out feature for all users.

  You must manually enter this parameter and value to the `[general]` section of the `opentext.ini` file.

- **Syntax:**

  `DisableSelectReservedBy=FALSE`

- **Values:**

  `TRUE` or `FALSE`. Setting this parameter to `FALSE` enables the group check-out feature for all users.

  By default, this parameter is not displayed in the `opentext.ini` file, which is the equivalent of setting the parameter to `FALSE`.

DisplayServerName

- **Description:**

The user-friendly name given to the server.

OpenText recommends that you modify this value using the **Configure Server Parameters** page, rather than edit the `opentext.ini` file directly. For more information, see “Site Name” in “Configuring Basic Server Parameters” on page 73.

- **Syntax:**

  `DisplayServerName=<my_server_name>`

- **Values:**

  A string of up to 64 alphanumeric characters. By default, this parameter is not displayed in the `opentext.ini` file until you enter a value in the **Site Name** field.

DocModTimeInDays

- **Description:**

  Number of days for which the **Modified** icon appears beside Content Server items that are modified.

  OpenText recommends that you modify this value using the **Configure Server Parameters** page, rather than edit the `opentext.ini` file directly. For more information, see “Duration of New and Modified Indicators” in “Configuring Basic Server Parameters” on page 73.

- **Syntax:**

  `DocModTimeInDays=7`

- **Values:**

  An integer greater than, or equal to, zero. The default value is `7`.

  If you set this value to `0`, zero, modified objects are not marked with the **Modified** icon.

DocNewTimeInDays

- **Description:**

  Number of days for which the **New** icon appears beside newly added Content Server items.

  OpenText recommends that you modify this value using the **Configure Server Parameters** page, rather than edit the `opentext.ini` file directly. For more information, see “Duration of New and Modified Indicators” in “Configuring Basic Server Parameters” on page 73.

- **Syntax:**

  `DocNewTimeInDays=2`

- **Values:**

  An integer greater than, or equal to, zero. The default value is `2`.

If you set this value to `0`, zero, new objects are not marked with the **New** icon.

EnableAutoRestarts

- **Description:**

  If `EnableAutoRestarts` is set to `FALSE`, Content Server does not automatically restart. When the **Restart Content Server** page appears (after installation of a module, for example), you must restart Content Server using the operating system.

  If `EnableAutoRestarts` is set to `TRUE`, you are offered a choice when the **Restart Content Server** page appears. You can let Content Server restart automatically, or you can bypass the automatic restart and restart Content Server using the operating system.

  You must manually enter this parameter and value to the `[general]` section of the `opentext.ini` file.

- **Syntax:**

  ```
  EnableAutoRestarts=TRUE
  ```

- **Values:**

  `TRUE` or `FALSE`. By default, this parameter does not appear in the `opentext.ini` file, which is equivalent to `EnableAutoRestarts=TRUE`.

ExplorerServerName

- **Description:**

  This value is only set if you install the Explorer module; it stores the display name for the Explorer server.

  Warning

  Do not manually change the value of `ExplorerServerName`.

- **Syntax:**

  `ExplorerServerName=`*`<Explorer_server_display_name>`*

- **Values:**

  By default, this parameter is displayed in the `opentext.ini` file with a null value, `ExplorerServerName=`, until you install the Explorer module.

HaveSeenLicenseSetupPage

- **Description:**

  Indicates that the **License Setup** page was displayed during the initial setup of Content Server.

  Important

  OpenText recommends that you do not manually change the value of `HaveSeenLicenseSetupPage`.

- **Syntax:**

  ```
  HaveSeenLicenseSetupPage=TRUE
  ```

- **Values:**

  `TRUE` or `FALSE`. This value is set during installation. If you completed the installation and setup of Content Server, this parameter will be `TRUE`.

HaveSeenModuleInstallPage

- **Description:**

  Indicates that the **Install Modules** page was displayed during the initial setup of Content Server.

  > **Important**
  > OpenText recommends that you do not manually change the value of `HaveSeenModuleInstallPage`.

- **Syntax:**

  ```
  HaveSeenModuleInstallPage=TRUE
  ```

- **Values:**

  `TRUE` or `FALSE`. This value is set during installation. If you completed the installation and setup of Content Server, this parameter will be `TRUE`.

HaveSeenSetupPage

- **Description:**

  Indicates that the **Setup** page was displayed during the initial setup of Content Server.

  > **Important**
  > OpenText recommends that you do not manually change the value of `HaveSeenSetupPage`.

- **Syntax:**

  ```
  HaveSeenSetupPage=TRUE
  ```

- **Values:**

  `TRUE` or `FALSE`. This value is set during installation. If you completed the installation and setup of Content Server, this parameter will be `TRUE`.

HaveValidatedDBAdminServers

- **Description:**

  Indicates that the database administration servers have been validated during the initial setup of Content Server.

Important
OpenText recommends that you do not manually change the value of `HaveValidatedDBAdminServers`.

- **Syntax:**

  ```
  HaveValidatedDBAdminServers=TRUE
  ```

- **Values:**

  `TRUE` or `FALSE`. This value is set during installation. If you completed the installation and setup of Content Server, this parameter will be `TRUE`.

HaveValidatedEnterpriseDataSource

- **Description:**

  Indicates that the Enterprise data source has been validated during the initial setup of Content Server.

  Important
  OpenText recommends that you do not manually change the value of `HaveValidatedEnterpriseDataSource`.

- **Syntax:**

  ```
  HaveValidatedEnterpriseDataSource=TRUE
  ```

- **Values:**

  `TRUE` or `FALSE`. This value is set during installation. If you completed the installation and setup of Content Server, this parameter will be `TRUE`.

HaveValidatedFacetsVolume

- **Description:**

  Indicates that the Facets Volume has been validated during the initial setup of Content Server.

  Important
  OpenText recommends that you do not manually change the value of `HaveValidatedFacetsVolume`.

- **Syntax:**

  ```
  HaveValidatedFacetsVolume=TRUE
  ```

- **Values:**

  `TRUE` or `FALSE`. This value is set during installation. If you completed the installation and setup of Content Server, this parameter will be `TRUE`.

HaveValidatedReSyncPage

- **Description:**

Indicates that the resynchronize page has been validated during the initial setup of Content Server.

> **Important**
> OpenText recommends that you do not manually change the value of `HaveValidatedReSyncPage`.

- **Syntax:**

  `HaveValidatedReSyncPage=TRUE`

- **Values:**

  `TRUE` or `FALSE`. This value is set during installation. If you completed the installation and setup of Content Server, this parameter will be `TRUE`.

HaveValidatedSearchComponents

- **Description:**

  Indicates that the search components have been validated during the initial setup of Content Server.

> **Important**
> OpenText recommends that you do not manually change the value of `HaveValidatedSearchComponents`.

- **Syntax:**

  `HaveValidatedSearchComponents=TRUE`

- **Values:**

  `TRUE` or `FALSE`. This value is set during installation. If you completed the installation and setup of Content Server, this parameter will be `TRUE`.

HaveValidatedWarehouseVolume

- **Description:**

  Indicates that the Warehouse Volume has been validated during the initial setup of Content Server.

> **Important**
> OpenText recommends that you do not manually change the value of `HaveValidatedWarehouseVolume`.

- **Syntax:**

  `HaveValidatedWarehouseVolume=TRUE`

- **Values:**

  `TRUE` or `FALSE`. This value is set during installation. If you completed the installation and setup of Content Server, this parameter will be `TRUE`.

HTMLCharset

- **Description:**

  By default, Content Server does not specify a character set encoding; the character set used depends on the configuration of each user's web browser. You can set Content Server to override the web browser's setting with a different character set.

- **Syntax:**

  `HTMLCharset=<character_set>`

- **Values:**

  Any character encoding that is recognized by Content Server-supported web browsers. This parameter does not have a default value and is not displayed in the `opentext.ini` file by default.

htmlImagePrefix

- **Description:**

  The URL prefix, or alias, in your HTTP server that is mapped to the directory containing image files and other support files, such as Java applets and Content Server's online help files.

  OpenText recommends that you modify this value using the **Configure Server Parameters** page, rather than edit the `opentext.ini` file directly. For more information, see “URL Prefix for /support Directory” in “Configuring Basic Server Parameters” on page 73.

- **Syntax:**

  `htmlImagePrefix=/img/`

- **Values:**

  A URL prefix defined in your HTTP server. The default value is `/<cgi_URL_prefix>/support/`, where *<cgi_URL_prefix>* is the URL prefix of the `<Content_Server_home>/cgi` directory, and *<Content_Server_home>* is the root of your Content Server installation.

InstallAdminPort

- **Description:**

  The TCP/IP port on which the Admin server accepts connections during installation. This value is set by the Content Server installation program, based on the Admin server port number entered when Content Server was installed.

- **Syntax:**

  `InstallAdminPort=5858`

- **Values:**

  Any open TCP/IP port. The default value is `5858`. This value is set during installation, and is not used once the installation is finished.

integrity

- **Description:**

  An parameter used by the database verification process. The database verification process sets `integrity=TRUE` when it starts and sets `integrity=FALSE` when it completes.

  Warning

  Do not manually change the value of `integrity`.

- **Syntax:**

  ```
  integrity=TRUE
  ```

- **Values:**

  `TRUE` or `FALSE`. The default value is `TRUE`. This value is set during installation.

LLIndexHTMLFile

- **Description:**

  Specifies the name of the HTML file used to generate the **About Content Server** page. A path is not required.

- **Syntax:**

  ```
  LLIndexHTMLFile=llindex.html
  ```

- **Values:**

  The name of a valid WebLingo HTML file. The default value is `llindex.html`.

LLIndexRequiresLogin

- **Description:**

  Specifies whether you need to log in to Content Server to view the **About Content Server** page.

  If `LLIndexRequiresLogin` is set to `FALSE`, users do not need to log in to view the **About Content Server** page. All other log-in security remains in place.

- **Syntax:**

  ```
  LLIndexRequiresLogin=FALSE
  ```

- **Values:**

  `TRUE` or `FALSE`. The default value is `FALSE`. This value is set during installation.

LogConfigPath

- **Description:**

  The directory in which the `contentserver.logging.properties` file is located. The `contentserver.logging.properties` file contains settings the govern the generation of Content Server log files.

OpenText recommends that you modify logging settings on the **Configure Log Settings** page, rather than by editing the `opentext.ini` file. For more information, see "Configuring Log Settings" on page 33.

- **Syntax:**

  ```
  LogConfigPath=.\config\contentserver.logging.properties
  ```

- **Values:**

  A directory path relative to the root of the Content Server installation. The default value is *<Content_Server_home>*`\config\`.

Logpath

- **Description:**

  The directory to which log files are written.

- **Syntax:**

  ```
  Logpath=.\logs\
  ```

- **Values:**

  A directory path relative to the root of the Content Server installation. The default value is `.\logs\`

MacBinaryDefault

- **Description:**

  This parameter applies to Macintosh workstations using Netscape browsers only. Specifies the default state of the **MacBinary (set before selecting a file)** check box on certain document upload pages.

  Setting this value to `TRUE` instructs Netscape browsers to encode the file to be uploaded in MacBinary format.

  You must manually enter this parameter and value to the `[general]` section of the `opentext.ini` file.

- **Syntax:**

  ```
  MacBinaryDefault=FALSE
  ```

- **Values:**

  `TRUE` or `FALSE`. The default value is `FALSE`, the check box is not selected. Also by default, the `MacBinaryDefault` parameter does not appear in the `opentext.ini` file, which is equivalent to `MacBinaryDefault=FALSE`.

MailtoAddressSeparator

- **Description:**

  The character that Content Server inserts between multiple recipient addresses in message composition windows.

OpenText recommends that you modify this value using the **Configure Server Parameters** page, rather than edit the `opentext.ini` file directly. For more information, see “Multiple Address Separator for ‘mailto:’ URL” in “Configuring Basic Server Parameters” on page 73.

- **Syntax:**

  ```
  MailtoAddressSeparator=,
  ```

- **Values:**

  A semi-colon (`;`) or a comma (`,`). The default value is a comma.

MaxListingOnGroupExpn

- **Description:**

  Maximum number of users to display when opening the members of a group. If you search for groups and then click a group to display its members, the maximum number of members displayed on the page is defined by the value of the `MaxListingOnGroupExpn` parameter.

- **Syntax:**

  ```
  MaxListingOnGroupExpn=100
  ```

- **Values:**

  An integer greater than, or equal to, zero. The default value is `100`.

MaxUsersToListPerPage

- **Description:**

  Maximum number of users or groups to be displayed on the results page when searching for users or groups.

- **Syntax:**

  ```
  MaxUsersToListPerPage=30
  ```

- **Values:**

  An integer greater than, or equal to, zero. The default value is `30`.

MessageClearInterval

- **Description:**

  The `MessageClearInterval` parameter sets the maximum number of days that Content Server stores Content Server Notification messages.

  If a user enables e-mail delivery of a Notification report, the messages associated with the report are cleared from the database when the e-mail message is sent. However, if a user does not enable e-mail delivery of a given Notification report, events corresponding to the interests of the report are stored in the database until the user opens and deletes them on the **Notification** tab of the Personal Workspace. If users are negligent in checking their **Notification** tabs, a lot of messages can accumulate in the database. To prevent an excessive amount of messages from accumulating, Content Server deletes all stored Notification reports that are older than the number of days set by the `MessageClearInterval` parameter.

- **Syntax:**

  ```
  MessageClearInterval=30
  ```

- **Values:**

  Any whole number of days. The default value is `30`.

NavigationOption

- **Description:**

  Governs whether navigation menus and icons in the Content Server user interface are Java-enabled.

- **Syntax:**

  ```
  NavigationOption=0
  ```

- **Values:**

  Valid values are: `0`, `1`, or `2`. The default value is `0`.

Value	Description
0	This is the default value. Sets Java-enabled navigation as the default condition but allows individual users to choose non-Java navigation.
1	Sets non-Java navigation only for all users.
2	Sets non-Java navigation as the default condition but allows individual users to choose Java-enabled navigation.

NewsDftExpiration

- **Description:**

  Number of days before a News item expires. If you set this value to `0`, zero, News items do not expire.

- **Syntax:**

  ```
  NewsDftExpiration=2
  ```

- **Values:**

  An integer greater than, or equal to, zero. The default value is `2`.

NTPATH

- **Description:**

Path to the directory containing the document-viewing filters. This path is appended to the host's path environment variable. The path is set during installation.

- **Syntax:**

  ```
  NTPATH=C:\OPENTEXT\filters\
  ```

- **Values:**

  An absolute path, including trailing slash. The default value is `*<Content_Server_home>*\filters\`, where *<Content_Server_home>* is the root of your Content Server installation.

NTSERVICENAME

- **Description:**

  This parameter applies to Windows workstations only. This parameter indicates the service name of this particular Content Server instance in the Windows Services dialog box. This value is set during installation.

- **Syntax:**

  ```
  NTSERVICENAME=OTCS
  ```

- **Values:**

  Any unique service name. The default value is `OTCS`.

NumOldLogs

- **Description:**

  This parameter, when added to the `[general]` section, determines the number of log files you want saved. When you restart the server, this parameter deletes all old threads. This parameter does not impact connect logs.

- **Syntax:**

  ```
  NumOldLogs=1
  ```

- **Values:**

  An integer greater than, or equal to, zero. The default value is `1`.

Value	Description
`0`	Sets Content Server to display only the current set of thread logs.
`1`	Displays the current set of thread logs, and saves the next oldest set. This is the default value.
<n>	Any number that represents the number of log files, in addition to the one displayed, that you want saved.

OTHOME

- **Description:**

  The full path to the root of the Content Server installation. The placeholder, <*Content_Server_home*>, is used to refer to this root directory.

- **Syntax:**

  ```
  OTHOME=C:\OPENTEXT\
  ```

- **Values:**

  An absolute path is required. On Windows systems, `C:\OPENTEXT\` is an example of the value of `OTHOME`. On Linux systems, `/usr/local/` is an example of the value of `OTHOME`. This value is set during installation.

PauseSleep

- **Description:**

  The length of time, in microseconds, each item in a News player remains on screen.

- **Syntax:**

  ```
  PauseSleep=2000
  ```

- **Values:**

  Any integer greater than, or equal to, zero. The default value is `2000`, or `0.002` seconds.

Port

- **Description:**

  The port that clients use to connect to the server.

- **Syntax:**

  ```
  Port=2099
  ```

- **Values:**

  Any open TCP/IP port. The default value is `2099`.

Profile

- **Description:**

  Enables the OScript profiler, which can be used by software developers to analyze the behavior of Content Server software.

  The OScript profiler creates a profile data file in the *`<Content_Server_home>`* `\logs\` folder for each running Content Server thread.

Profile data files follow a naming convention of `profile-<process_id>-<thread_id>.<extension>`, where *<extension>* could be `csv`, `out`, `csv.zip`, or `out.zip`. (See "ProfileFormat" on page 161.) For example, a profile data file could have the name `profile-2620-7003.csv.zip`.

Note: If the `Profile` parameter is enabled under the `[general]` section name, the profiler generates a profile data file for every Content Server OScript thread.

You can also enable `Profile` under different section names to restrict its effects. If `Profile` is enabled under `[llserver]`, Content Server worker threads are profiled. If `Profile` is enabled in one or more agent sections (for example, `[wfagent]` or `[daagent]`), only the agent functions are profiled.

- **Syntax:**

  ```
  Profile=0
  ```

- **Values:**

  Valid values are `0`, `1`, or `2`. The default value is `0`.

Value	Description
0	Disabled. If the `Profile` parameter does not appear in the `opentext.ini` file, it is equivalent to `Profile=0`. This is the default value.
1	Only OScript function calls are profiled.
2	OScript function calls and built-in function calls are profiled.

ProfileFormat

- **Description:**

  Specifies the file format of profiler output. Applies only if "Profile" on page 160 is enabled (set to 1 or 2).

- **Syntax:**

  ```
  ProfileFormat=out.zip
  ```

- **Values:**

  Valid values are `out`, `csv`, `out.zip`, or `csv.zip`. The default value is `out.zip`.

  out
  Callgrind format. Callgrind (http://valgrind.org/docs/manual/cl-format.html) is an open-source format that can be viewed using kcachegrind (http://kcachegrind.sourceforge.net/html/Home.html) and other tools.

  csv
  Comma-separated values.

out.zip
Compressed (gzip) Callgrind format.

csv.zip
Compressed (gzip) comma-separated values.

ScheduleHandlerClearInterval

- **Description:**

  The number of days after which all unprocessed events will be cleared.

  OpenText recommends that you modify this value using the **Clear Outstanding Events** page, rather than edit the `opentext.ini` file directly.

  You access the **Clear Outstanding Events** page from the **Content Server Administration** page. In the **Notification Administration** section, click **Configure Clear Outstanding Events**. For more information, see *OpenText Content Server - Notifications Administration (LLESWBN-AGD)*.

- **Syntax:**

  ```
  ScheduleHandlerClearInterval=30
  ```

- **Values:**

  Any integer greater than, or equal to, zero. The default value is `30`.

Server

- **Description:**

  The name of the host on which the server resides. This parameter is used in conjunction with the "Port" on page 160 parameter to enable clients to connect to the server.

- **Syntax:**

  ```
  Server=localhost
  ```

- **Values:**

  A fully-qualified hostname or an IP address. The default value is `localhost`.

UploadDirectory

- **Description:**

  The `UploadDirectory` parameter is used to restrict the location from which Content Server accepts Documents for upload. If specified, Content Server will only upload Documents found in this directory.

  OpenText recommends that you modify this value using the **Configure Server Parameters** page, rather than edit the `opentext.ini` file directly. For more information, see "Upload Directory" in "Configuring Basic Server Parameters" on page 73.

- **Syntax:**

```
UploadDirectory=C:\upload\
```

- **Values:**

  This parameter does not have a default value and is not displayed in the `opentext.ini` file until you enter a value in the **Upload Directory** field.

version

- **Description:**

  File version identifier.

  Important
  OpenText recommends that you do not manually change the value of `version`.

- **Syntax:**

  ```
  version=22
  ```

- **Values:**

  This entry does not have a default value.

7.3.27 [HelpMap]

- **Description:**

  The `[HelpMap]` section contains mappings for Content Server's context-sensitive online help for users. A help mapping creates a link between a keyword that identifies a page of the Content Server interface, for example, the Personal Workspace or Search page, and the name of an HTML online help page.

  Help mappings for functions available only to the Administrator, or users with system administration rights, are found in the "[AdminHelpMap]" on page 97 section.

  Important
  OpenText recommends that you do not change the default mappings in the `opentext.ini` file.

7.3.28 [HHExcludedMimeTypes]

- **Description:**

  The entries in the `[HHExcludedMimeTypes]` section determine which types of items are excluded from being hit highlighted in Content Server. If you add a MIME type to this section, the **Hit Highlight** command will not be available in the **Functions** menu for the corresponding item type.

The entries in the `[HHIncludedMimeTypes]` section, which determines the types of items that can be hit highlighted in Content Server, takes precedence over the entries in the `[HHExcludedMimeTypes]` section. However, if the `[HHIncludedMimeTypes]` section is not included or is empty in the `opentext.ini` file, Content Server uses the `[HHExcludedMimeTypes]` section to determine which items can be hit highlighted. For information about the `[HHIncludedMimeTypes]` section, see "[HHIncludedMimeTypes]" on page 166.

- **Syntax:**

  ```
  mime1=image/jpeg
  ```

- **Values:**

  Each entry in the `[HHExcludedMimeTypes]` section has the following format: `mime`*`<n>`*`=`*`<mimetype>`*, where *`<n>`* is a unique number.

  You must specify MIME types using the correct format. The following table lists some common MIME types:

- application/activemessage
- application/andrew-inset
- application/applefile
- application/atomicmail
- application/dca-rft
- application/dec-dx
- application/mac-binhex40
- application/macwriteii
- application/msword
- application/news-message-id
- application/news-transmission
- application/octet-stream
- application/oda
- application/pdf
- application/postscript
- application/powerpoint
- application/remote-printing
- application/rtf
- application/slate
- application/vnd.lotus-1-2-3
- application/vnd.lotus-freelance
- application/vnd.ms-excel
- application/vnd.ms-powerpoint
- application/vnd.ms-project
- application/vnd.ms-tnef
- application/wita
- application/wordperfect5.1
- application/x-ami
- application/x-amipro
- application/x-bcpio
- application/x-cpio
- application/x-csh
- application/x-dvi
- application/x-gtar
- application/x-latex
- application/x-macbinary
- application/x-mif
- application/x-netcdf
- application/x-outlook
- application/x-quattro
- application/x-quattropro
- application/x-quattroproj
- application/x-sh
- application/x-shar
- application/x-sv4cpio
- application/x-sv4crc
- application/x-tar
- application/x-tcl
- application/x-tex
- application/x-texinfo
- application/x-troff
- application/x-troff-man
- application/x-troff-me
- application/x-troff-ms
- application/x-ustar
- application/x-wais-source
- application/x-wordperfect
- application/x-wordperfectmac
- application/x-wordperfect4.2
- application/x-wordperfect5e
- application/x-wordperfect5.1j
- application/x-wordperfect6.0
- application/x-wordperfect6e
- application/x-wordperfect6.1
- application/x-wordperfect7
- application/x-zip-compressed
- application/zip
- audio/basic
- image/gif
- image/ief
- image/jpeg
- image/tiff
- image/x-cmu-raster
- image/x-portable-anymap
- image/x-portable-bitmap
- image/x-portable-graymap
- image/x-portable-pixmap
- image/x-rgb
- image/x-xbitmap
- image/x-xpixmap
- image/x-xwindowdump
- message/external-body
- message/news
- message/partial
- message/rfc822
- message/alternative
- multipart/
- multipart/appledouble
- multipart/digest
- multipart/mixed
- multipart/parallel
- text/html
- text/plain
- text/richtext
- text/tab-separated-values
- text/xml
- text/x-setext
- text/x-sgml
- video/mpeg
- video/quicktime
- video/x-msvideo
- video/x-sgi-movie

• application/x-hdf • application/x-js-taro	• audio/x-aiff • audio/x-wav	

7.3.29 [HHIncludedMimeTypes]

- **Description:**

  The entries in the `[HHIncludedMimeTypes]` section determine which types of items can be hit highlighted in Content Server. Only items that match the MIME types in this section have the **Hit Highlight** command available in their **Functions** menu in Content Server. The `[HHIncludedMimeTypes]` section takes precedence over the `[HHExcludedMimeTypes]` section, which determines which types of items are excluded from being hit highlighted in Content Server. However, if the `[HHIncludedMimeTypes]` section is not included or is empty in the `opentext.ini` file, Content Server uses the `[HHExcludedMimeTypes]` section to determine which items can be hit highlighted. For information about the `[HHExcludedMimeTypes]` section, see "[HHExcludedMimeTypes]" on page 163.

- **Syntax:**

  ```
  mime1=image/jpeg
  ```

- **Values:**

  Each entry in the `[HHIncludedMimeTypes]` section has the following format: `mime<n>=<mimetype>`, where `<n>` is a unique number.

  You must specify MIME types using the correct format. To view some common MIME types, see the table located in "[HHExcludedMimeTypes]" on page 163.

7.3.30 [HitHighlight]

The `[HitHighlight]` section contains the configuration settings for hit highlighting, and for Content Server 16.0, some cache related settings also apply to View as Web Page. Hit highlighting allows users to highlight the instances of their search terms within a particular search result item. For more information, see *OpenText Content Server - Search (LLESWBB-UGD)*.

Before Content Server can hit highlight a search result item, it converts the item to HTML using a Document Conversion Server process, if the converted content is not located in the front end cache or Admin Server File Cache.

The `[HitHighlight]` section contains the following parameters:

Important

OpenText strongly recommends that you do not modify the values of these parameters:

• "cacheMaintenanceMins" on page 167 • "cachePath" on page 167	• "cacheSize" on page 167 • "cacheSizeMax" on page 167	• "HHStyle" on page 168

cacheMaintenanceMins

- **Description:**

  Specifies the interval between cache maintenance activities which trim the front end cache to the number of entries defined for the `cacheSize` parameter.

- **Syntax:**

  ```
  cacheMaintenanceMins=10
  ```

- **Values:**

  An integer greater than, or equal to, zero. By default, this parameter is not included in the `opentext.ini` file, which is equivalent to `cacheMaintenanceMins=10`.

cachePath

- **Description:**

  Specifies the front end cache directory which stores files converted for Hit Highlighting and View as Web Page.

- **Syntax:**

  ```
  <Content_Server_home>\cache\hh\
  ```

- **Values:**

  An absolute path. The default is `<Content_Server_home>\cache\hh\`, where *<Content_Server_home>* is the root of your Content Server installation.

cacheSize

- **Description:**

  Specifies the number of page file entries that are cached for the Hit highlighting and View as Web Page functions. This is needed to prevent the local Hit highlighting cache directory from storing too many entries.

- **Syntax:**

  ```
  cacheSize=10
  ```

- **Values:**

  An integer greater than, or equal to, zero. By default, this parameter is not included in the `opentext.ini` file, which is equivalent to `cacheSize=10`.

cacheSizeMax

- **Description:**

  Specifies the number of page files at which to begin deleting View as Web Page files to reduce the total to the value defined by the `cacheSize` parameter. This is needed to prevent the local Hit highlighting cache directory from storing too many entries.

- **Syntax:**

  ```
  cacheSizeMax=(2 * cacheSize)
  ```

- **Values:**

  An integer greater than, or equal to, zero. By default, this parameter is not included in the `opentext.ini` file, which is equivalent to `cacheSizeMax=(2 * cacheSize)`. This means two times the `cacheSize` parameter value.

HHStyle

- **Description:**

  Specifies the background color, font color, font size, font style, and font weight used when hit highlighting a key word or phrase. An example of font style is italic. An example of font weight is bold.

- **Syntax:**

  ```
  HHStyle={background:red; color:blue}
  ```

- **Values:**

  The values that you specify for this parameter must be contained in braces, `{}`. Each entry takes the form *`<option>`*`:`*`<value>`*. Entries are separated by semicolons.

  The `HHStyle` parameter can contain five display options: `background`, `color`, `font-size`, `font-style` or `font-weight`. The values of each element are described in the following table:

Option	Value
background	Any valid HTML color. A color is a either a color name or a numerical RGB specification. For more information, consult an HTML color reference chart or website.
color	Any valid HTML color. A color is a either a color name or a numerical RGB specification. For more information, consult an HTML color reference chart or website.
font-size	An integer representing the absolute font size
font-style	One of three possible values: `normal`, `italic`, or `oblique`, depending on the font family used.

Option	Value
font-weight	One of the following values: • normal • bold • bolder • lighter • 100 • 200 • 300 • 400 • 500 • 600 • 700 • 800 • 900 The values `100-900` represent an ordered sequence, where each number indicates a weight that is at least as dark as the previous value. The value `normal` is equal to `400`, and `bold` is equal to `700`.

7.3.31 [Home]

By default, the `[Home]` section does not appear in the `opentext.ini` file. You only need to add it if you want to change the default value of the `EditOrganizeMaxItems` parameter, which is described below.

EditOrganizeMaxItems

- **Description:**

  Sets the maximum number of items that Content Server displays per page when a user is editing/organizing items, such as favorites or Projects on tabs.

  For example, if a user is a member of 150 Projects, and clicks the **Edit/Organize** link when opening the **All** Projects tab in their Personal Workspace, Content Server only displays the first 100 Project names on the first page. To see the remaining 50 Project names, the user must click **2 of 2** in the **Page** list at the bottom of the page.

- **Syntax:**

  ```
  EditOrganizeMaxItems=100
  ```

- **Values:**

  An integer greater than, or equal to, `0`. The default is `100`.

7.3.32 [IndexObject]

The `[IndexObject]` section contains OpenText proprietary information.

Important
OpenText recommends that you do not change any of the options in this section.

7.3.33 [InterestsProfile]

The `[InterestsProfile]` section controls the configuration parameter for **Report Settings** in **Notification Administration**. To set this parameter, OpenText recommends that you use the Configure Notification page, rather than edit the `opentext.ini` file directly.

EventNo

- **Description:**

  Limits Content Server to processing only this number of events per cycle.

- **Syntax:**

  `EventNo=1000`

- **Values:**

  An integer greater than, or equal to, zero.

  The default value is `1000`.

7.3.34 [ipmove]

The `[ipmove]` section is used to control whether an item is sent to a particular iPool.

Note: There is a separate configuration file to set all arguments, for example, `\bin\ipmove -inifile opentext.ini -config myconfig`, where `myconfig` is a file in the same format as a standard initialization file. To set `[ipmove]` parameters, OpenText recommends that you use the `myconfig` file, rather than edit the `opentext.ini` file directly. For details, see *OpenText Content Server - Administering Search (LLESWBS-AGD)*.

readfields

- **Description:**

  The `readfields` parameter works, when there is more than one write iPool, with the location specified in the **File Path** field, in the **Non-EFS Object Content** section of the Setting Extractor General Settings page. For details, see *OpenText Content Server - Administering Search (LLESWBS-AGD)*.

  If a directory path location is specified for the **File Path** field, the original path name is passed to the first iPool. Any other iPools which get this item also get a copy of the temporary file specified in the **File Path** field. It is the consumer iPool's responsibility to delete the temporary file when it has consumed the content and committed the transaction.

If an output iPool is not selected, and `readfields` is not set, then copying of the temporary file specified in the **File Path** location will **not** occur. This is because iPool messages are fast copied and there is no entry parsing. The potential failure to delete the temporary file could happen with a Two Way Tee process, or with a Merge.

- **Syntax:**

  `readfields=TRUE`

- **Values:**

  `TRUE` or `FALSE`. The default value is `FALSE`.

  Setting `readfields=TRUE` is only required if there are no patterns, and more than one output is specified. If you specify a pattern, `readfields=TRUE` is set automatically.

7.3.35 [javaserver]

The `[javaserver]` section allows you to modify the settings of the Virtual Machine, VM, running in Content Server. You can optimize performance of the Java web application server by typing more VM arguments. For example:

```
JavaVMOption_4=-Xms256M
JavaVMOption_5=-Xmx256M
```

Note: On a multi-processor 64 bit server, the Java process uses more memory for each additional cpu in use. To limit the amount of memory used by the javaserver upon a Content Server startup, add the following to the [javaserver] section of the `opentext.ini` file: `JavaVMOption_5=Xmx256M`.

For information about more arguments you can use, locate your Java SDK installation, then navigate to `<`*`Java_SDK_installation_path`*`>\jre\bin\client\Xusage.txt`. The text file lists and explains each argument.

7.3.36 [Lang_xx_XX]

The `[Lang_`*`<xx>`*`_`*`<XX>`*`]` section, where *<xx>_<XX>* indicates the locale of your Content Server version, controls how Content Server deals with dates, times, and user names that are subject to locale settings. The following Content Server Administration pages describe changes you can make to the `[Lang_`*`<xx_XX>`*`]` section:

- “Setting Date and Time Formats” on page 30
- “To Configure User Name Display” on page 428

This page contains information about the following parameters:

ENV_NLS_COMP

- **Description:**

  Sets the Oracle National Language Support (NLS) collation setting (which specifies how Oracle performs comparisons) used by an Oracle Content Server database. If this setting does not appear in the `opentext.ini` file, an Oracle Content Server database uses the existing settings of your Oracle server.

- **Syntax:**

  ```
  ENV_NLS_COMP=LINGUISTIC
  ```

- **Values:**

  One of `BINARY`, `LINGUISTIC`, or `ANSI`. The Oracle default value is `LINGUISTIC`.

ENV_NLS_SORT

- **Description:**

  Sets the Oracle National Language Support (NLS) sort setting (which specifies how Oracle sorts the results of `ORDERBY` queries) used by an Oracle Content Server database. If this value is not set, an Oracle Content Server database uses the existing settings of your Oracle server.

  By default, Oracle performs case-sensitive sorting and comparisons, if you want Content Server to behave in a case-insensitive manner, set the `ENV_NLS_SORT` setting to a case-insensitive setting, such as `GENERIC_M_CI`. With this setting in place, Content Server would treat `MyDocument` and `mydocument` as the same name and would not permit items with these names to be added to the same container.

- **Syntax:**

  ```
  ENV_NLS_SORT=GENERIC_M_CI
  ```

- **Values:**

  `BINARY`, or any linguistic definition name allowed by Oracle

InputDateFormat

- **Description:**

Specifies how input fields appear for the day, month, and year. Other characteristics are governed by the InputDateSeqFormat parameter. For more information, see “Input Date” in “Setting Date and Time Formats” on page 30.

- **Syntax:**

  ```
  InputDateFormat=%m/%d/%Y
  ```

- **Values:**

  The default setting is a two-digit month, the day, and the year: `%m/%d/%Y`.

InputDateSeqFormat

- **Description:**

  Specifies the order in which input fields appear for the day, month, and year, and what characters separate the elements of the date. Other characteristics are governed by the TwoDigitYears parameter. For more information, see “Input Date” in “Setting Date and Time Formats” on page 30.

- **Syntax:**

  ```
  InputDateSeqFormat={1,1,2,1,'/','/'}
  ```

- **Values:**

  The default setting is month, day, and year, all separated by a slash: `{1,1,2,1,'/','/'}`.

InputTimeFormat

- **Description:**

  Specifies whether Content Server accepts time inputs in 12-hour format, for example `02:41 PM`, or 24-hour format, for example `14:41`. For more information, see “Time Zone” in “Setting Date and Time Formats” on page 30.

- **Syntax:**

  ```
  InputTimeFormat=%I:%M %p
  ```

- **Values:**

  The default setting is a 12-hour format: `%I:%M %p`.

LongDateFormat

- **Description:**

  Specifies how Content Server displays the day, month, and year. Other characteristics are governed by the LongDateSeqFormat parameter. For more information, see “Setting Date and Time Formats” on page 30.

- **Syntax:**

  ```
  LongDateFormat=%m/%d/%Y
  ```

- **Values:**

The default setting is a two-digit month, the day, and the year: `%m/%d/%Y`.

LongDateSeqFormat

- **Description:**

  Specifies the order in which input fields appear for the day, month, and year, and what characters separate the elements of the date. Other characteristics are governed by the TwoDigitYears parameter. For more information, see "Setting Date and Time Formats" on page 30.

- **Syntax:**

  ```
  LongDateSeqFormat={1,1,2,1,'/','/'}
  ```

- **Values:**

  The default setting is month, day, and year, all separated by a slash: `{1,1,2,1,'/','/'}`.

LongTimeFormat

- **Description:**

  Specifies whether Content Server displays times in 12-hour format, for example `02:41 PM`, or 24-hour format, for example `14:41`. For more information, see "Setting Date and Time Formats" on page 30.

- **Syntax:**

  ```
  LongTimeFormat=%I:%M %p
  ```

- **Values:**

  The default setting is a 12-hour format: `%I:%M %p`.

ShortDateFormat

- **Description:**

  Specifies how Content Server displays the day, month, and year. Other characteristics are governed by the ShortDateSeqFormat parameter. For more information, see "Setting Date and Time Formats" on page 30.

- **Syntax:**

  ```
  ShortDateFormat=%m/%d/%Y
  ```

- **Values:**

  The default setting is a two-digit month, the day, and the year: `%m/%d/%Y`.

ShortDateSeqFormat

- **Description:**

  Specifies the order in which Content Server displays the day, month, and year, and what characters separate the elements of the date. Other characteristics are governed by the TwoDigitYears parameter. For more information, see "Setting Date and Time Formats" on page 30.

- **Syntax:**

  ```
  ShortDateSeqFormat={1,1,2,1,'/','/'}
  ```

- **Values:**

  The default setting is month, day, and year, all separated by a slash: `{1,1,2,1,'/','/'}`.

ShortTimeFormat

- **Description:**

  Specifies whether Content Server displays times in 12-hour format, for example `02:41 PM`, or 24-hour format, for example `14:41`. For more information, see "Setting Date and Time Formats" on page 30.

- **Syntax:**

  ```
  ShortTimeFormat=%I:%M %p
  ```

- **Values:**

  The default setting is a 12-hour format: `%I:%M %p`.

UserNameDisplayFormat

- **Description:**

  A format in which a Content Server user's name displays throughout Content Server, in fields such as **Created by**, **Owned by**, and **User**.

  OpenText recommends that you only modify this value using the **Configure User Name Display** page, rather than edit the `opentext.ini` file directly. For more information, see "Display Name Format" in "To Configure User Name Display" on page 428.

- **Syntax:**

  ```
  UserNameDisplayFormat=1
  ```

- **Values:**

  Valid values are:

  - `1`, which displays the Log-in ID. This is the default value.
  - `2`, which displays FirstName LastName.
  - `3`, which displays FirstName MiddleInitial. LastName.
  - `4`, which displays LastName, FirstName.
  - `5`, which displays LastName, FirstName MiddleInitial.
  - `6`, which displays LastName FirstName.

7.3.37 [llserver]

The `[llserver]` section contains settings that determine the number of threads that Content Server uses in its operation. Although you can edit these settings directly, OpenText recommends that you change the number of threads on the **Configure Performance Settings** administration page. For more information, see "Configuring Performance Settings" on page 76

Increasing the number of threads allows Content Server to serve a greater number of users, until the capacity of the Content Server host computer is reached. The more threads you allow, the more system resources Content Server consumes.

Note: The `opentext.ini` file installed by Content Server 10.5 SP1 and later contains the `number` setting instead of the `min` and `max` settings.

- If you perform a new installation of Content Server 10.5 SP1 and later, the `number` setting appears in this section, but the `min` and `max` settings do not.
- If you perform a new installation of Content Server 10.5 Update 2014–09 or earlier, the `min` and `max` settings appear in this section but the `number` setting does not.

id

- **Description:**

  This is OpenText proprietary information.

max

- **Description:**

  This setting is used if the `number` setting does not appear in the `[llserver]` section. Content Server sets the number of threads to the value of `min` or `max`. It uses whichever value is greater.
- **Syntax:**

  `max=8`
- **Values:**

  An integer greater than or equal to `1`.

min

- **Description:**

  This setting is used if the `number` setting does not appear in the `[llserver]` section. Content Server sets the number of threads to the value of `min` or `max`. It uses whichever value is greater.
- **Syntax:**

  `min=8`

- **Values:**

  An integer greater than, or equal to, `1`.

number

- **Description:**

  The number of threads that Content Server uses. If this setting does not appear in the `[llserver]` section, Content Server uses the `min` and `max` settings to determine the number of threads to use.

- **Syntax:**

  ```
  number=8
  ```

- **Values:**

  An integer greater than, or equal to, `1`. The default value is `8`.

path

- **Description:**

  This is OpenText proprietary information.

Profile

- **Description:**

  Enables the OScript profiler, which can be used by software developers to analyze the behavior of Content Server software. For more information, see “Profile” on page 160

7.3.38 [llview]

In the `[llview]` section, you can correct problems of excess resource consumption by `llview` processes. These processes are created every time a user opens a document in Content Server.

CancelTimeOut

- **Description:**

  Instructs Content Server to end any `llview` process that exceeds the stated number of seconds.

- **Syntax:**

  ```
  CancelTimeOut=10
  ```

- **Values:**

  Any integer greater than, or equal to, `0`.

7.3.39 [loader]

The `[loader]` section contains proprietary OpenText information.

Important
OpenText recommends that you do not change any of the options in this section.

7.3.40 [Modules]

- **Description:**

  The `[Modules]` section contains module information. The values in this section are set by Content Server and by the modules themselves.

  Important
  OpenText recommends that you do not modify any of the settings in this section.

- **Values:**

  There are three lines for each module. For example, the following is the module definition for the Discussions module:

  - `ospaces_discussion={'discussion'}. . .`
  - `module_11=discussion. . .`
  - `discussion=_3_0_0`

  The first line lists the OSpaces which make up the module. This is a comma-separated list of one or more *OSpace* names. Each name must be delimted by apostrophes, and the entire list must be contained in braces: `{'`*`<value>`*`', '`*`<value>`*`'}`.

  The second line is used to help iterate through the list of installed modules.

  The third line defines the module's version number.

7.3.41 [nlqsearch]

Content Server's Natural Language Query system uses the functionality provided by the Content Server Summarizer to parse the text that users enter when submitting natural language queries. The `[nlqsearch]` section contains most of the same parameters that appear in the `[Summarizer]` section; however, the default values of these parameters may differ.

The `[nlqsearch]` section of the `opentext.ini` file contains the following parameters:

SumAbbrevFile

- **Description:**

  Specifies the abbreviation file that the Content Server Summarizer uses to define common abbreviations and all three-letter combinations that are not words.

- **Syntax:**

  ```
  SumAbbrevFile=../config/abbrev.eng
  ```

- **Values:**

  A relative path and file name. By default, the abbreviation file is named `abbrev.eng` and is stored in the config directory of your Content Server installation. For example, *`<Content_Server_home>`*`/config`, where *<Content_Server_home>* is the root of your Content Server installation.

SumDefFile

- **Description:**

  Specifies the definition file that the Content Server Summarizer uses to define its operation. The definition file contains five numbers, one number per line, each representing the following:

  - A score multiplier for sentences that are in the first 20 percent of a document. These sentences are probably introductory sentences and are likely to be good summary sentences.
  - A maximum number of word tokens allowed in a summary sentence. A word token is a combination of letters, numbers, dashes, and entity references. The Summarizer marks sentences containing more word tokens than the maximum number as unreadable and does not use them as summary sentences.
  - A minimum number of word tokens allowed in a summary sentence. The Summarizer marks sentences containing fewer word tokens than the minimum number as unreadable and does not use them as summary sentences.
  - A maximum ratio of non-word tokens to word tokens. If the actual ratio of non-word tokens to word tokens exceeds this number, the Summarizer marks the sentence as unreadable and does not use it as a summary sentence.
  - The number of documents used to form the data for the statistical significance of words in the word frequency file.

- **Syntax:**

  ```
  SumDefFile=../config/natlang.eng
  ```

- **Values:**

  A path, relative to the value of the `otpath` parameter in the `[OTCommon]` section of the `opentext.ini` file. By default, the definition file is named `natlang.eng` and is stored in the config directory of your Content Server installation. For example, *`<Content_Server_home>`*`/config`, where *<Content_Server_home>* is the root of your Content Server installation.

SumDocFreqFile

- **Description:**

  Specifies the word frequency file that contains the data necessary for the Content Server Summarizer to calculate the statistical significance of words in documents. This file contains a list of words that occurred in more than 1,000 of the 1,371,876 documents that OpenText used to build the statistical background for the Summarizer's default settings.

- **Syntax:**

  ```
  SumDocFreqFile=../config/docfreq.eng
  ```

- **Values:**

  A relative path and file name. By default, the word frequency file is named `docfreq.eng` and is stored in the config directory of your Content Server installation. For example, *`<Content_Server_home>`*`/config`, where *<Content_Server_home>* is the root of your Content Server installation.

SumStopWordFile

- **Description:**

  Specifies the stopword file that the Content Server Summarizer uses to define a list of common stopwords. Stopwords are words that add no semantic value to a sentence. These words are typically functional words such as *a*, *and*, and *the*. By distinguishing stopwords from semantically important words, the Content Server Summarizer identifies which words are more likely to contribute to the document's distinct meaning, increasing the accuracy of its summaries and key phrases.

- **Syntax:**

  ```
  SumStopWordFile=../config/nlstopword.eng
  ```

- **Values:**

  A relative path and file name. By default, the stopword file is named `nlstopword.eng` and is stored in the config directory of your Content Server installation. For example, *`<Content_Server_home>`*`/config`, where *<Content_Server_home>* is the root of your Content Server installation.

SumTagFile

- **Description:**

Specifies the tag file that contains a list of markup tags that appear in documents. Examples of markup tags include HTML, XML, and SGML. Next to each tag is a number that specifies the tag's importance to the Content Server Summarizer.

Range of Tag Significance Settings table:

Number	Label	Description
0	IGNORE_TAG	The Summarizer ignores these tags, but does not ignore the data enclosed in them. If a sentence begins before this tag, and has this tag within it, the Summarizer does not break the sentence into two sentences. By default, unknown tags are marked with this number.
1	SENTENCE_BREAKING_IGNORE_TAG	The Summarizer ignores these tags, but does not ignore the data enclosed in them. If a sentence begins before this tag, and has this tag within it, the Summarizer breaks the sentence into two sentences.
2	IGNORE_BETWEEN_TAGS	The Summarizer ignores these tags and the data enclosed in them.
3	ABSTRACT	This value marks the data enclosed in these tags as abstract, or overview, sentences. The Summarizer uses sentences in the title, abstract, and conclusion, in that order, before any other sentences to create the summary.
4	CONCLUSION	This value marks the data enclosed in these tags as concluding sentences. The Summarizer uses sentences in the title, abstract, and conclusion, in that order, before any other sentences to create the summary.
5	TITLE_MAJOR	This value marks the data enclosed in these tags as title sentences. The Summarizer uses sentences in the title, abstract, and conclusion, in that order, before any other sentences to create the summary.

- **Syntax:**

```
SumTagFile=../config/tags.eng
```

- **Values:**

  A relative path and file name. By default, the tag file is named `tags.eng` and is stored in the config directory of your Content Server installation. For example, `<Content_Server_home>/config`, where <*Content_Server_home*> is the root of your Content Server installation.

7.3.42 [notify]

The `[notify]` section contains proprietary OpenText information.

Important
OpenText recommends that you do not change any of the options in this section.

7.3.43 [options]

You can set several logging options in the `[options]` section, and enable or disable some key functionality, such as the search engine and Content Server Notification. The following Content Server Administration pages describe changes you can make to the `[options]` section:

- "Configuring Performance Settings" on page 76
- *OpenText Content Server - Notifications Administration (LLESWBN-AGD)*
- *OpenText Content Server - Administering Search (LLESWBS-AGD)*

This page contains information about the following parameters:

- "EFSCopyBufferSize" on page 182
- "EnableAgents" on page 183
- "EnableAgentsTestAll" on page 183
- "EnableAgentsTrace" on page 183
- "EnableNotification" on page 184
- "excludeNodeIDs" on page 184
- "MaxOpenSessions" on page 184
- "maxRightsString" on page 185
- "processAllNodeIds" on page 185
- "wantByteServing" on page 185
- "wantDebugSearch" on page 185
- "wantLAPILogs" on page 186
- "wantLogs" on page 186
- "wantSearchLogs" on page 186
- "wantSecureCookies" on page 186
- "wantTimings" on page 187
- "wantVerbose" on page 187
- "wantWeb" on page 187

EFSCopyBufferSize

- **Description:**

  Sets the file buffer size for files that are copied to and from the External File Storage.

  OpenText recommends that you only modify this value using the **Configure Performance Settings** page, rather than edit the `opentext.ini` file directly. For more information, see "File Buffer Size" in "Configuring Performance Settings" on page 76.

- **Syntax:**

  `EFSCopyBufferSize=<value_in_bytes>`

- **Values:**

  A value in bytes, between 16384 and 2097152. The default value is `524288` (500 KB).

EnableAgents

- **Description:**

  This is OpenText proprietary information.

  > **Important**
  > OpenText recommends that you do not manually change the value of `EnableAgents`.

- **Syntax:**

  `EnableAgents=TRUE`

- **Values:**

  `TRUE` or `FALSE`. The default value is `TRUE`.

EnableAgentsTestAll

- **Description:**

  This is OpenText proprietary information.

  > **Important**
  > OpenText recommends that you do not manually change the value of `EnableAgentsTestAll`.

- **Syntax:**

  `EnableAgentsTestAll=FALSE`

- **Values:**

  `TRUE` or `FALSE`. The default value is `FALSE`.

EnableAgentsTrace

- **Description:**

  This is OpenText proprietary information.

  > **Important**
  > OpenText recommends that you do not manually change the value of `EnableAgentsTestAll`.

- **Syntax:**

  `EnableAgentsTestAll=FALSE`

- **Values:**

  `TRUE` or `FALSE`. The default value is `FALSE`.

EnableNotification

- **Description:**

  Enables or disables Content Server Notification.

  OpenText recommends that you only modify this value using the **Configure Notification** page, rather than edit the `opentext.ini` file directly. For more information, see “Enable Notifications” in *OpenText Content Server - Notifications Administration (LLESWBN-AGD)*.

- **Syntax:**

  `EnableNotification=FALSE`

- **Values:**

  `TRUE` or `FALSE`. The default value is `FALSE` until Content Server Notification is enabled by the Administrator.

excludeNodeIDs

- **Description:**

  Allows you to specify node IDs so that they are excluded from processing when adding documents to Content Server.

- **Syntax:**

  `excludeNodeIDs=`*`<nodeID1>`*, *`<nodeId2>`*

- **Values:**

  A comma separated list of <*NodeID*>'s.

You can force the system to ignore the `excludeNodeIDs` parameter by setting the “processAllNodeIds” on page 185 parameter to `TRUE`.

MaxOpenSessions

- **Description:**

  This setting defines the maximum number of user log-in sessions cached on a server thread.

  OpenText recommends that you only modify this value using the **Configure Performance Settings** page, rather than edit the `opentext.ini` file directly. For more information, see “Number of Sessions” in “Configuring Performance Settings” on page 76.

- **Syntax:**

  `MaxOpenSessions=100`

- **Values:**

An integer greater than, or equal to, zero. The default value is `100`.

maxRightsString

- **Description:**

  This parameter specifies which of two methods Content Server should use to calculate a user's permissions for a particular item being requested. The choice is based on the number of user rights that the user has. If a user who is attempting to access an item in Content Server has a number of rights lists greater than, or equal to, the specified number, the *threshold*, Content Server calculates the user's permissions set for that item in a different way. The alternative method is intended to improve performance in cases where individual Content Server users have a large number of individual rights.

- **Syntax:**

  ```
  maxRightsString=250
  ```

- **Values:**

  An integer greater than, or equal to, zero. The default value is `250`.

processAllNodeIds

- **Description:**

  Set `processAllNodeIds` to `TRUE` if you want the system to ignore the "excludeNodeIDs" on page 184 parameter.

  By default, this entry is not displayed in the `opentext.ini` file until it is set, which is equivalent to `processAllNodeIds=FALSE`.

- **Syntax:**

  ```
  processAllNodeIds=FALSE
  ```

- **Values:**

  `TRUE` or `FALSE`. The default value is `FALSE`.

wantByteServing

- **Description:**

  Enables or disables byte serving of PDF files.

- **Syntax:**

  ```
  wantByteServing=FALSE
  ```

- **Values:**

  `TRUE` or `FALSE`. The default value is `FALSE`.

wantDebugSearch

Reserved for use by the **Configure Log Settings** page.

wantLAPILogs

- **Description:**

  Sets whether or not Content Server records the LAPI `inArgs` and `outArgs` values, which are received and sent by the server, to the thread logs. For more information, see *OpenText Content Server - Notifications Administration (LLESWBN-AGD)*.

  To enable this feature, you must manually add `wantLAPILogs=TRUE` to the `opentext.ini` file in the `[options]` section.

- **Syntax:**

  ```
  wantLAPILogs=FALSE
  ```

- **Values:**

  `TRUE` or `FALSE`. By default, the `wantLAPILogs` parameter does not appear in the `opentext.ini` file, which is equivalent to `wantLAPILogs=FALSE`.

wantLogs

- **Description:**

  Turns detailed connection logging on or off. Log output is written to files called `connect`*<n>*`.log`, where *<n>* is the thread number. For more information, see *OpenText Content Server - Administering Search (LLESWBS-AGD)*.

- **Syntax:**

  ```
  wantLogs=FALSE
  ```

- **Values:**

  `TRUE` or `FALSE`. The default value is `FALSE`.

wantSearchLogs

- **Description:**

  Enables or disables search transaction logging. Input, or queries, and output, or results, from the search engine, `otsearch`, are logged. Transactions are logged to the file `search.log` in the *`<Content_Server_home>`*`/logs` directory, where *<Content_Server_home>* is the root of your Content Server installation. For more information, see *OpenText Content Server - Administering Search (LLESWBS-AGD)*.

- **Syntax:**

  ```
  wantSearchLogs=FALSE
  ```

- **Values:**

  `TRUE` or `FALSE`. The default value is `FALSE`.

wantSecureCookies

- **Description:**

If Content Server is running on an HTTPS server, SSL, the secure flag will be set for the user's login cookie.

- **Syntax:**

  ```
  wantSecureCookies=TRUE
  ```

- **Values:**

  `TRUE` or `FALSE`. The default value is `TRUE`.

wantTimings

- **Description:**

  Records transaction timings in the thread logs. For more information, see *OpenText Content Server - Administering Search (LLESWBS-AGD)*.

- **Syntax:**

  ```
  wantTimings=TRUE
  ```

- **Values:**

  `TRUE` or `FALSE`. The default value is `TRUE`.

wantVerbose

- **Description:**

  Records all arguments passed from the web browser to the server in the thread logs. For more information, see *OpenText Content Server - Administering Search (LLESWBS-AGD)*.

- **Syntax:**

  ```
  wantVerbose=TRUE
  ```

- **Values:**

  `TRUE` or `FALSE`. The default value is `TRUE`.

wantWeb

- **Description:**

  Enables Content Server to run on the web. If you plan to use Content Server only through LAPI, you can set `wantWeb` to `FALSE`.

- **Syntax:**

  ```
  wantWeb=TRUE
  ```

- **Values:**

  `TRUE` or `FALSE`. The default value is `TRUE`.

7.3.44 [OTAdmin]

The `[OTAdmin]` section defines a port number for connection requests.

port

- **Description:**

  Specifies the port on which the admin server accepts connection requests.

  You must modify the value of this parameter in the `opentext.ini` file. For more information, see "Understanding the opentext.ini File" on page 93.

- **Syntax:**

  ```
  port=5858
  ```

- **Values:**

  Any open TCP/IP port. The default value is `5858`.

7.3.45 [OTCommon]

InstallType

- **Description:**

  This is OpenText proprietary information

otpath

- **Description:**

  The path to the directory containing the configuration files for indexing and searching.

- **Syntax:**

  ```
  otpath=C:\OPENTEXT\config
  ```

- **Values:**

  An absolute path.

7.3.46 [Passwords]

Important
All password settings with the exception of "ChangePWAtFirstLogin" on page 190 are now deprecated, and are controlled in OpenText Directory Services. For more information, see *OpenText Directory Services - Installation and Administration Guide (OTDS-IWC)*.

This page contains information about the following parameters:

• “MinimumLength” on page 189 • “MustContainDigits” on page 189	• “ExpirationDays” on page 189 • “ChangePWAtFirstLogin” on page 190	• “MustBeDifferent” on page 190 • “preventPwdReuse” on page 190

These parameters appear in the [Passwords] section by default. To set them, and with the exception of “ChangePWAtFirstLogin” on page 190, you need to access the Directory Services user interface. For more information, see *OpenText Content Server - Administering OpenText Directory Services Integration Administration (LLESDSI-AGD)* and *OpenText Directory Services - Installation and Administration Guide (OTDS-IWC)*.

MinimumLength

- **Description:**

  Minimum number of characters required for a user's password. Deprecated as of Content Server 16.0.0.

- **Syntax:**

  ```
  MinimumLength=0
  ```

- **Values:**

  An integer between 0 and 16. The default value is 0. If 0 is selected, a blank password is acceptable. The maximum value is `16`.

MustContainDigits

- **Description:**

  Governs whether or not passwords must contain at least one numeric character. Deprecated as of Content Server 16.0.0.

- **Syntax:**

  ```
  MustContainDigits=FALSE
  ```

- **Values:**

  `TRUE` or `FALSE`. The default value is `FALSE`, which means that a numeric character is required.

ExpirationDays

- **Description:**

  The number of days after which user passwords expire. Deprecated as of Content Server 16.0.0.

- **Syntax:**

  ```
  ExpirationDays=-1
  ```

- **Values:**

  An integer greater than or equal to `-1`. The default value is `-1`. A value of `-1` indicates that passwords never expire.

ChangePWAtFirstLogin

- **Description:**

  Governs whether or not users must change their passwords after logging in to Content Server the first time.

- **Syntax:**

  ```
  ChangePWAtFirstLogin=TRUE
  ```

- **Values:**

  `TRUE` or `FALSE`. The default value is `TRUE`, which means that users must change their passwords after they first log-in to Content Server.

MustBeDifferent

- **Description:**

  Governs whether or not users must specify a new password when they change their password. Deprecated as of Content Server 16.0.0.

- **Syntax:**

  ```
  MustBeDifferent=FALSE
  ```

- **Values:**

  `TRUE` or `FALSE`. The default value is `FALSE`, which means that the changed password can be the same as the previous password.

preventPwdReuse

- **Description:**

  Determines how many days must pass before a previously used password can be reused. Deprecated as of Content Server 16.0.0.

- **Syntax:**

  ```
  preventPwdReuse=0
  ```

- **Values:**

  An integer 0 or greater. The default value is `0`. A value set to 0 indicates that the same password can be used immediately.

7.3.47 [Project]

By default, the [Project] section does not appear in the opentext.ini file. You only need to add it if you want to change the default value of the ProjectOutlineSubtypes parameter, which is described below.

ProjectOutlineSubtypes

- **Description:**

  By default, Content Server Projects contain seven subtypes of WebNode objects. The subtype values translate to a node type name, or a label, which gets included in the **Include Item Types** field on the **Project Outline** page of a Project.

  By adding such a [Project] section to the opentext.ini file, the Administrator can change subtype values based on your organization's project needs.

- **Syntax:**

  ```
  ProjectOutlineSubtypes={204,215,207,144,140,136,400,0}
  ```

- **Values:**

  The default values are:

Node Subtype Value	Node Type
204	Task List
215	Discussion
207	Channel
144	Document
140	URL
136	Compound Document
0	Folder

For a complete list of node type number to name mappings, see “Node Type Number to Name Mappings” on page 94.

7.3.48 [QDF]

The settings in the [QDF] section control the configuration of the Quality Document Filters, QDFs, that the Document Conversion Service, DCS, uses. The QDFs convert documents from their native formats to HTML or plain text for viewing and indexing purposes. The details of this conversion process vary, depending on the native file format. For example, the QDFs convert Microsoft Outlook files to HTML or plain text for indexing. If available, the QDFs use the Unicode version of a Microsoft Outlook file by default; however, if the Unicode format is not available, the QDFs use the RTF version. If neither the Unicode nor the RTF versions are available, the QDFs use the HTML version. If neither the Unicode, nor the RTF, nor the HTML versions are available, the QDFs use a plain-text version. In cases where the QDFs use the RTF or HTML version of a Microsoft Outlook file for indexing, the content is extracted and returned to the DCS as if it were an attachment. The QDFs RTF filtering mechanism then converts the RTF content to HTML or plain text for indexing. For more information about QDFs, see *OpenText Content Server - Administering Search (LLESWBS-AGD)*.

The `[QDF]` section also configures the extraction of custom OLE document properties from supported Microsoft Office documents. The exported metadata region names are identical to the OLE document property names, with two exceptions: they have the prefix `OTDoc` and discard all whitespace and slash characters.

The `[QDF]` section of the `opentext.ini` file contains information about the following parameters:

- “DefaultLatinEncoding” on page 192
- “lib” on page 192
- “showcdata” on page 193
- “maxfilesunzip” on page 193
- “MinAsianAvgLength” on page 193
- “MinAsianTextRatio” on page 194
- “MinAsianTokens” on page 194
- “MinHighLowRatioForEUC” on page 195
- “MinHighLowRatioForSJIS” on page 195
- “outputoleinfo” on page 196
- “x-maxcalls” on page 197
- “x-timeout” on page 198

DefaultLatinEncoding

- **Description:**

  Specifies the default Latin character set to detect.

  A character set can have multiple mappings. For example, the ISO-8859-* and EUC character sets each have several regional variations. Because these variations overlap significantly, you can specify the default character set that the QDFs will detect.

- **Syntax:**

  ```
  DefaultLatinEncoding=ISO-8859-1
  ```

- **Values:**

  `ISO-8859-1` ~ `ISO-8859-15`, `WinANSI`. By default, this parameter does not appear in the opentext.ini file, which is equivalent to `DefaultLatinEncoding=ISO-8859-1`.

lib

- **Description:**

  Specifies the name of the library to be loaded by the DCS. A library is a list of operations associated with a conversion filter that the DCS reads to perform the conversion. This parameter is a required setting for the DCS.

  Modifying the value of this parameter may prevent the DCS from functioning, or from functioning properly.

Important
Do not modify the value of this parameter unless directed to do by OpenText Customer Support.

- **Values:**

  The default value is `dcsqdf`.

showcdata

- **Description:**

  Specifies whether CDATA sections in Extensible Markup Language, XML, documents should be extracted so that they can be indexed by the DCS.

- **Syntax:**

  ```
  showcdata=FALSE
  ```

- **Values:**

  `TRUE` or `FALSE`, where `FALSE` instructs the DCS to omit CDATA sections when extracting data from XML documents so that they can be indexed. The default value is `FALSE`.

  Note: Setting this parameter to `TRUE` may affect search performance.

maxfilesunzip

- **Description:**

  Specifies the maximum number of files that the QDFs extract from a compressed file during conversion. The files that are extracted are determined by the order in which the file creator originally added them.

  Note: Recursive processing of compressed files is supported by the DCS rules file configuration. That is, an LZH file within an LZH file, or a ZIP file within an LZH file.

- **Syntax:**

  ```
  maxfilesunzip=250
  ```

- **Values:**

  A positive integer. The default value is `250`.

MinAsianAvgLength

- **Description:**

  Specifies the minimum average run length of adjacent multibyte tokens.

  Once the QDFs have determined that a file does not contain only 7-bit characters, Asian character set detection typically occurs. If the value of the `MinHighLowRatioForSJIS` or `MinHighLowRatioForEUC` parameters is satisfied, the QDFs will scan some text to determine the character set in use.

When scanning multibyte text, the QDFs perform some additional text evaluations. For example, the QDFs determine the average run length of adjacent multibyte tokens to determine whether the scanned text contains actual Asian text or just instances of some tokens. In order to be evaluated, the average run length of adjacent tokens must be longer than the minimum value set for the `MinAsianAvgLength` parameter.

Note: When determining the average run length of adjacent multibyte tokens, the QDFs ignore all white space in the scanned text.

For more information about the additional conditions that must be satisfied for mulitbyte text evaluation to occur, see the `MinAsianTextRatio` and `MinAsianTokens` parameters.

- **Syntax:**

  `MinAsianAvgLength=6`

- **Values:**

  An integer greater than `1`. The default value is `6`.

MinAsianTextRatio

- **Description:**

  Specifies the percentage of bytes of Asian text that must be exceeded during Asian text detection.

  Once the QDFs have determined that a file does not contain only 7-bit characters, Asian character set detection typically occurs. If the value of the `MinHighLowRatioForSJIS` or `MinHighLowRatioForEUC` parameters is satisfied, the QDFs will scan some text to determine the character set in use.

  When scanning multibyte text, the QDFs perform some additional text evaluations. First, the QDFs determine the average run length of adjacent multibyte tokens. For more information, see the `MinAsianAvgLength` parameter. Then, one or both of the following conditions must be satisfied:

  - The percentage of bytes of Asian tokens in the text exceeds the value specified by the `MinAsianTextRatio` parameter.
  - The number of identified tokens exceeds the value specified by the `MinAsianTokens` parameter. For more information, see the `MinAsianTokens` parameter.

- **Syntax:**

  `MinAsianTextRatio=50`

- **Values:**

  An integer between `1` and `100`. The default value is `50`.

MinAsianTokens

- **Description:**

Specifies the number of multibyte tokens that must be identified during Asian text detection.

Once the QDFs have determined that a file does not contain only 7-bit characters, Asian character set detection typically occurs. If the value of the `MinHighLowRatioForSJIS` or `MinHighLowRatioForEUC` parameters is satisfied, the QDFs will scan some text to determine the character set in use.

When scanning multibyte text, the QDFs perform some additional text evaluations. First, the QDFs determine the average run length of adjacent multibyte tokens. For more information, see the `MinAsianAvgLength` parameter. Then, one or both of the following conditions must be satisfied:

- The percentage of bytes of Asian tokens in the text exceeds the value specified by the `MinAsianTextRatio` parameter. For more information, see the `MinAsianTextRatio` parameter.
- The number of identified tokens exceeds the value specified by the `MinAsianTokens` parameter.

- **Syntax:**

  `MinAsianTokens=5000`

- **Values:**

  An integer greater than `0`. The default value is `5000`.

MinHighLowRatioForEUC

- **Description:**

  Specifies the ratio of high to low bytes that must be exceeded in order for Asian character set detection to occur in EUC files.

  Once the QDFs have determined that a file does not contain only 7-bit characters, Asian character set detection typically occurs. This level of character set detection can be time consuming and may delay the MIME type detection operations. So, depending on the content of the documents at your Content Server site, you may not want this level of detection to occur or may only want it to occur when a certain ratio of high to low byte characters is exceeded within a document. You can manipulate this ratio by changing the value of the `MinHighLowRatioForEUC` parameter.

- **Syntax:**

  `MinHighLowRatioForEUC=60`

- **Values:**

  An integer between `1` and `100`. The default value is `60`.

MinHighLowRatioForSJIS

- **Description:**

  Specifies the ratio of high to low bytes that must be exceeded in order for Asian character set detection to occur in Shift-JIS files.

Once the QDFs have determined that a file does not contain only 7-bit characters, Asian character set detection typically occurs. This level of character set detection can be time consuming and may delay the MIME type detection operations. So, depending on the content of the documents at your Content Server site, you may not want this level of detection to occur or may want it to occur only when a certain ratio of high to low byte characters is exceeded within a document. You can manipulate this ratio by changing the value of the `MinHighLowRatioForSJIS` parameter.

- **Syntax:**

  ```
  MinHighLowRatioForSJIS=50
  ```

- **Values:**

  An integer between `1` and `100`. The default value is `50`.

outputoleinfo

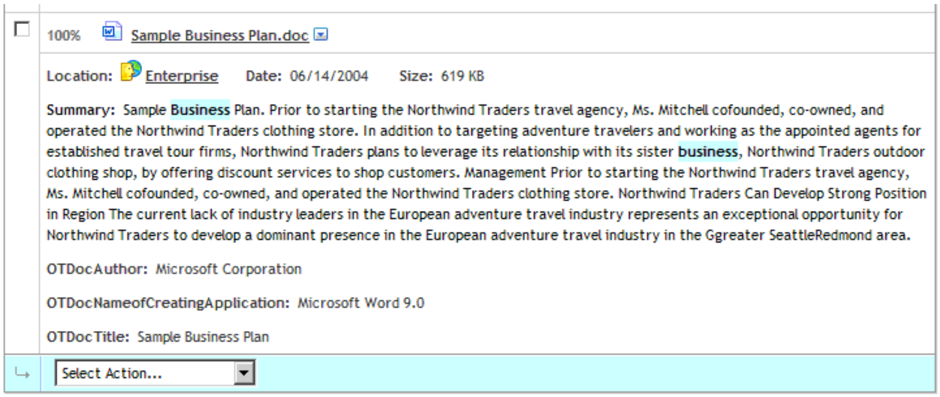
- **Description:**

  Specifies whether the QDFs should extract OLE properties from the document and export these properties as Content Server metadata regions. OLE is a program-integration technology that is supported by all Microsoft Office programs. OLE allows information to be shared among different programs.

  If this parameter is enabled, the QDFs extract the standard OLE properties as well as any custom OLE properties associated with a document. The standard OLE properties are extracted and exported as the following metadata regions in Content Server:

  - OTDocTitle
  - OTDocSubject
  - OTDocAuthor
  - OTDocKeywords
  - OTDocComments
  - OTDocTemplate
  - OTDocLastSavedBy
  - OTDocRevisionNumber
  - OTDocTotalEditingTime
  - OTDocLastPrinted
  - OTDocCreateTimeDate
  - OTDocLastSavedTimeDate
  - OTDocNumberofPages
  - OTDocNumberofWords
  - OTDocNumberofCharacters
  - OTDocThumbnail
  - OTDocNameofCreatingApplication
  - OTDocSecurity
  - OTDocCategory
  - OTDocPresentationTarget
  - OTDocBytes
  - OTDocLines
  - OTDocParagraphs
  - OTDocSlides
  - OTDocNotes
  - OTDocHiddenSlides
  - OTDocMMClips
  - OTDocScaleCrop
  - OTDocHeadingPairs
  - OTDocTitlesofParts
  - OTDocManager
  - OTDocCompany
  - OTDocLinksUpToDate

  The following is an example of exported metadata regions displayed in a search result:



□ 100% Sample Business Plan.doc

Location: Enterprise Date: 06/14/2004 Size: 619 KB

Summary: Sample Business Plan. Prior to starting the Northwind Traders travel agency, Ms. Mitchell cofounded, co-owned, and operated the Northwind Traders clothing store. In addition to targeting adventure travelers and working as the appointed agents for established travel tour firms, Northwind Traders plans to leverage its relationship with its sister business, Northwind Traders outdoor clothing shop, by offering discount services to shop customers. Management Prior to starting the Northwind Traders travel agency, Ms. Mitchell cofounded, co-owned, and operated the Northwind Traders clothing store. Northwind Traders Can Develop Strong Position in Region The current lack of industry leaders in the European adventure travel industry represents an exceptional opportunity for Northwind Traders to develop a dominant presence in the European adventure travel industry in the Ggreater SeattleRedmond area.

OTDocAuthor: Microsoft Corporation

OTDocNameofCreatingApplication: Microsoft Word 9.0

OTDocTitle: Sample Business Plan

- **Syntax:**

  `outputoleinfo=TRUE`

- **Values:**

  `TRUE` or `FALSE`, where `TRUE` instructs a QDF to extract the OLE-embedded metadata from the file. The default `opentext.ini` configuration file shipped with Content Server has a value of `TRUE`. The assumed default value, if not specified in the configuration file, is `FALSE`.

x-maxcalls

- **Description:**

  Specifies the number of times a worker process is reused for processing documents. During document conversion, the DCS loads a worker process. The worker process loads the appropriate conversion filter and uses it to convert the document. To increase performance, the DCS reuses the worker process for multiple conversions. If the worker process encounters an error, the process is stopped before reaching the value specified in the `opentext.ini` file.

  Important
  OpenText strongly recommends that you do not modify the value of this parameter.

- **Values:**

  The default value is inherited from the `maxcalls` parameter of the `[DCSworker]` section of the `opentext.ini` file.

  Note: The `x-maxcalls` parameter is only functional when the conversion filter it modifies is managed by a worker process. For more information about configuring a worker process, see *OpenText Content Server - Administering Search (LLESWBS-AGD)*.

  Specifying a value for `x-maxcalls` will override the value of `maxcalls` in the `[DCSworker]` section of the `opentext.ini` file.

x-timeout

- **Description:**

  Specifies the maximum number of seconds to wait before terminating a document conversion worker process. You configure this parameter when the default value specified in the `timeout` parameter is inappropriate. You configure the `timeout` parameter for each conversion filter. For example, some conversion filters convert documents more slowly than other conversion filters. In this case, the `timeout` default value of 30 seconds may not be applicable, as the average conversion time is longer than this value. In this case, you can modify the `x-timeout` value to a higher and more appropriate value.

  Important
  OpenText strongly recommends that you do not modify the value of this parameter.

- **Values:**

  The default value is inherited from the `timeout` parameter of the `[DCSworker]` section of the `opentext.ini` file.

  Note: The `x-timeout` parameter is only functional when the conversion filter it modifies is managed by a worker process. For more information about configuring a worker process, see *OpenText Content Server - Administering Search (LLESWBS-AGD)*.

  Specifying a value for `x-timeout` will override the value of `timeout` in the `[DCSworker]` section of the `opentext.ini` file.

7.3.49 [receiver_logs]

Contains settings that affect the generation of Content Server Receiver logs.

OpenText recommends that you modify the values in this section on the **Configure Log Settings** page, rather than by editing the `opentext.ini` file. For more information, see “Configuring Log Settings” on page 33.

logLevel

- **Description:**

  Enables or disables the generation of Receiver logs by setting the level of logging. You can specify a level of `0` (no logging), or `2` (logging enabled).

- **Syntax:**

  ```
  logLevel=2
  ```

- **Values:**

  Either 0 or 2. The default value is `2`.

7.3.50 [relagent]

The [relagent] section contains proprietary OpenText information.

> **Important**
> OpenText recommends that you do not change any of the options in this section.

7.3.51 [report]

The [report] section contains LiveReport options. In versions of Livelink prior to 8.1, this section was called [reports].

objectSubTypes

- **Description:**

  If you want to make changes to the settings of the objectSubTypes parameter, you should make those changes on the **Manage Object SubTypes** administrative page. For more information, see *OpenText Content Server - LiveReports Administration (LLESREP-AGD)*.

  The objectSubTypes parameter controls the Content Server object types that appear in **Object** input type lists in LiveReports. To modify the Content Server object types displayed in these lists, modify the list of node type numbers, also known as object type numbers.

  See "Node Type Number to Name Mappings" on page 94 if you need a reference for each object type.

  For more information about object subtypes, see the *Content Server Module Development Guide*, or inspect the LLNode and WebNode objects in the Content Server Builder.

- **Syntax:**

  ```
  objectSubTypes={ 299, 215, 202, 206, 204, 144, 0, 140, 207, 130, 1, 131,
  136, 400, 223, 230, 208, 128, 335 }
  ```

- **Values:**

  The default value for this parameter is:

  ```
  objectSubTypes={ 299, 215, 202, 206, 204, 144, 0, 140, 207, 130, 1, 131,
  136, 400, 223, 230, 208, 128, 335 }
  ```

  As shown in the example, the list of valid Content Server node type, or object type, numbers must be separated by commas and the entire list must be delimited by braces.

InsertStrEnabled

- **Description:**

  Enables and disables the InsertStr input type.

- **Syntax:**

```
InsertStrEnabled=false
```

- **Values:**

  true or false. The default value is `false`.

- **Example:**

  ```
  [report]
  InsertStrEnabled=true
  ```

blockedSQLterms

- **Description:**

  Specifies all terms that should be blocked from usage in SQL. These terms are checked whenever InsertStr has been used and the Secure mode enabled. For more information, see *OpenText Content Server - LiveReports (LLESREP-UGD)*.

- **Syntax:**

  ```
  blockedSQLterms=;,UPDATE,UPDATETEXT,WRITETEXT,REMOVE,DROP,CREATE,
  ALTER,INSERT,COMMIT,EXECUTE,FETCH,REVOKE,ROLLBACK,SAVE,TRUNCATE,
  UNION
  ```

- **Values:**

  A comma separated list of terms. The default value is `;,UPDATE,UPDATETEXT,WRITETEXT,REMOVE,DROP,CREATE, ALTER,INSERT,COMMIT,EXECUTE,FETCH,REVOKE,ROLLBACK,SAVE,TRUNCATE,UNION`.

ModificationSQLTerms

- **Description:**

  Specifies a list of terms that, if used in the SQL or in an SQL template, would require the user to set the **Allow Database Modification** option. For more information, see *OpenText Content Server - LiveReports (LLESREP-UGD)*.

- **Syntax:**

  ```
  ModificationSQLTerms=UPDATE,UPDATETEXT,WRITETEXT,REMOVE,DROP,
  CREATE,ALTER, INSERT,COMMIT,EXECUTE,FETCH,REVOKE,ROLLBACK,SAVE,
  TRUNCATE
  ```

- **Values:**

  A comma separated list of terms. The default value is `UPDATE,UPDATETEXT,WRITETEXT,REMOVE,DROP,CREATE,ALTER, INSERT,COMMIT,EXECUTE,FETCH,REVOKE,ROLLBACK,SAVE,TRUNCATE`.

AllowDBModification

- **Description:**

  Enables or disables the **Allow Database Modification** feature in LiveReports. For more information, see *OpenText Content Server - LiveReports (LLESREP-UGD)*.

- **Syntax:**

```
AllowDBModification=false
```

- **Values:**

  true or false. The default value is `false`.

  Note: This setting replaces a previous setting called `lockDBModification`. If you had previously set `lockDBModification=true`, that is now equivalent to the current `AllowDBModification=false`.

- **Example:**

  ```
  [report]
  AllowDBModification=true
  ```

QueryVisibleWithSeeContents

- **Description:**

  Determines whether the **View Query** option is available to users with only *See Contents* permission for the LiveReport. If the administrator sets this option to true, users with *See* and *See Contents* permissions on a LiveReport will be able to use the **View Query** option. For more information, see *OpenText Content Server - LiveReports (LLESREP-UGD)*.

- **Syntax:**

  ```
  QueryVisibleWithSeeContents=true
  ```

- **Values:**

  true or false. The default value is `true`.

- **Example:**

  ```
  [report]
  QueryVisibleWithSeeContents=false
  ```

7.3.52 [scheduleactivity]

This section contains proprietary OpenText information.

Warning

Do not manually change the values in the `scheduleactivity` section.

7.3.53 [SearchOptions]

The `[SearchOptions]` section contains the following Content Server Search parameters:

- "brokerObjectCacheExpire" on page 202
- "dateTypesAdditions" on page 202
- "defaultWebSearchDetail" on page 203
- "findSimilar" on page 203
- "functionMenu" on page 203
- "hitHighlight" on page 204
- "masterCacheDisable" on page 204
- "MaxImportAgentObjectsPerTransaction" on page 204
- "needValidHTTPSCerticate" on page 205
- "NoHiddenItemForResult" on page 205
- "objectTypes and objectTypesName" on page 205
- "redirectPost" on page 206
- "resultCountLookAhead" on page 207
- "TrueFileName" on page 207
- "wantMultipleEnterprise" on page 207

brokerObjectCacheExpire

- **Description:**

  Specifies the number of minutes that slice data on the Content Server search bar is cached before it is refreshed.

  For example, if you add or delete a slice, the `brokerObjectCacheExpire` parameter specifies the number of minutes that will elapse before the slice appears on, or is removed from, the Content Server search bar.

- **Syntax:**

  ```
  brokerObjectCacheExpire=5
  ```

- **Values:**

  An integer greater than, or equal to, zero. By default, this parameter is not included in the `opentext.ini` file, which is equivalent to `brokerObjectCacheExpire=5`. Setting the `brokerObjectCacheExpire` parameter to `0` specifies that slice data is not cached.

dateTypesAdditions

- **Description:**

  Specifies the list of non-default regions, additional ones discovered by the Search Index, that will be treated as dates by the System Attributes advanced search component. The date handling allows users to enter dates with a calendar widget instead of the special text syntax.

- **Syntax:**

  ```
  dateTypesAdditions={'region1name', 'region2name'}
  ```

- **Values:**

A comma separated list of any valid non-default regions. By default, this parameter does not appear in the `opentext.ini` file, which is equivalent to no regions specified.

An example of a valid entry is: `dateTypesAdditions={'OTEmailSentDate', 'OTEmailReceivedDate'}`

defaultWebSearchDetail

- **Description:**

  Specifies the initial state of the **Less Detail** and **More Detail** links for the **Web Search** and **Web Search —Themes Right Search Result** page styles. Users can change the initial state by specifying the other detail setting.

- **Syntax:**

  ```
  defaultWebSearchDetail=FALSE
  ```

- **Values:**

  `TRUE` or `FALSE`. By default, this parameter does not appear in the `opentext.ini` file, which is equivalent to `defaultWebSearchDetail=FALSE`, which sets the initial state to the **Less Detail** link. To set the initial state to the **More Detail** link, specify `defaultWebSearchDetail=TRUE`.

findSimilar

- **Description:**

  Specifies if the Find Similar option is disabled for search result items when using the search API with `outputformat=xml` (Extensible Markup Language). A temporary value for this parameter can also be set using search API parameters.

- **Syntax:**

  ```
  findSimilar=FALSE
  ```

- **Values:**

  `TRUE` or `FALSE`. Default is `TRUE`.

  Note: The values in the `opentext.ini` file are the defaults and if you set a value in the API parameters it will override the `opentext.ini` value. If no value is specified in either `opentext.ini` or the API parameter, the default value is `TRUE`.

functionMenu

- **Description:**

  Specifies if the Function menu is disabled for search result items when using the search API with `outputformat=xml` (Extensible Markup Language). A temporary value for this parameter can also be set using search API parameters.

- **Syntax:**

  ```
  functionMenu=false
  ```

- **Values:**

  `TRUE` or `FALSE`. Default is `TRUE`.

  > **Note:** The values in the `opentext.ini` file are the defaults and if you set a value in the API parameters it will override the `opentext.ini` value. If no value is specified in either `opentext.ini` or the API parameter, the default value is `TRUE`.

hitHighlight

- **Description:**

  Specifies if the hit highlighting option is disabled for search result items when using the search API with `outputformat=xml` (Extensible Markup Language). A temporary value for this parameter can also be set using search API parameters.

- **Syntax:**

  `hitHighlight=FALSE`

- **Values:**

  `TRUE` or `FALSE`. Default is `TRUE`.

  > **Note:** The values in the `opentext.ini` file are the defaults and if you set a value in the API parameters it will override the `opentext.ini` value. If no value is specified in either `opentext.ini` or the API parameter, the default value is `TRUE`.

masterCacheDisable

- **Description:**

  Specifies whether memory caching is prevented of search object data such as Search Manager region maps and slice definitions.

- **Syntax:**

  `masterCacheDisable=TRUE`

- **Values:**

  `TRUE` or `FALSE`. By default, this parameter does not appear in the `opentext.ini` file, which is equivalent to `masterCacheDisable=FALSE`.

MaxImportAgentObjectsPerTransaction

- **Description:**

  Specifies the maximum number of objects from the `DStagingImport` table to process per database transaction. This parameter can be used if there is a very large amount of data in the table, which may cause memory issues.

- **Syntax:**

  `MaxImportAgentObjectsPerTransaction=25`

- **Values:**

  An integer greater than or equal to `1`, or `-1` for unlimited. The default is `-1`. By default, this parameter does not appear in the `opentext.ini` file, which is equivalent to `MaxImportAgentObjectsPerTransaction=-1`.

needValidHTTPSCerticate

- **Description:**

  Specifies if a valid HTTPS (Hypertext Transfer Protocol Secure) certificate must be present for the URL to local file conversion to be able to retrieve a document over HTTPS.

- **Syntax:**

  ```
  needValidHTTPSCerticate=FALSE
  ```

- **Values:**

  `TRUE` or `FALSE`. Defaults to `FALSE`.

NoHiddenItemForResult

- **Description:**

  Specifies whether Hidden items appear in a search results list or not.

- **Syntax:**

  ```
  NoHiddenItemForResult=FALSE
  ```

- **Values:**

  `TRUE` or `FALSE`. By default, this parameter does not appear in the `opentext.ini` file, which is equivalent to `NoHiddenItemForResult=FALSE`, which includes items designated as Hidden in a search results list. To exclude Hidden items, specify `NoHiddenItemForResult=TRUE`.

objectTypes and objectTypesName

- **Description:**

  Determines which types of Content Server items appear in the **Object Type** list in the **System Attributes** section of the **Content Server Search** page. There are two parameters that control the **Object Type** list: `objectTypes` and `objectTypesName`.

  Together, these parameters allow you to map object subtype values to the display names that you want to appear in the **System Attributes** section's **Object Type** list. Arrange both `objectTypes` and `objectTypesName` in the order in which you want the options to appear in the **Object Type** list. If you want to add or remove an option from the **Object Type** list, you must add or remove the subtype value in the `objectTypes` parameter, and you must add or remove the corresponding display name from the `objectTypesName` parameter.

  For single known subtype values in the **Object Type** list, the corresponding `objectTypes` parameter is ignored in favour of the official object type name in

Content Server. This is done to ensure the type name is available in every user interface language.

Use the `objectTypes` parameter to list the subtype values of the Content Server item types that you want to appear in the **Object Type** list in the **System Attributes** section of the **Content Server Search** page. For example, in the default configuration, the node type `144`, (Content Server documents), corresponds to **Documents** in the **Object Type** list. You can also combine several subtype values by a Boolean OR operator to map them to the same option in the **Object Type** list. You must enclose such expressions in quotation marks within the `objectTypes` parameter. For example, in the default configuration, the entry `"130 OR 134"`, (Content Server topics and replies), corresponds to **Discussions** in the **Object Type** list. For a complete list of `subtype` values in your Content Server system, use the Content Server SDK Builder to run a script that lists all `subtype` values, or refer to "[llview]" on page 177.

Use the `objectTypesName` parameter to list the strings, enclosed in single quotation marks, that you want Content Server to display in the **Object Type** list for each entry in the `objectTypes` parameter. List the display names in the `objectTypesName` parameter in the same order as the `objectTypes` entries that they represent. By default, the 'All Types' parameter is applied.

Tip: You can change the language used for the `objectTypes` by entering an Xlate value instead of a numeric value.

- **Syntax:**

  ```
  objectTypes={144,0,"206|212|204|205","130|134|215",202,128,189}
  ```

  ```
  objectTypesName={'Documents','Folders','Tasks','Discussions',
  'Projects','Workflow Map','Workflow Status'}
  ```

- **Values:**

  By default, these parameters are not included in the `opentext.ini` file. This is the equivalent of the settings listed in the Syntax section above.

redirectPost

- **Description:**

  Specifies if search pages needing to "POST" search requests will redirect to a "GET" request so that the **Back** button in an internet browser will function as users expect it to. Also, the Content Server search bar will submit with a "GET" request when possible.

- **Syntax:**

  ```
  redirectPost=TRUE
  ```

- **Values:**

  `TRUE` or `FALSE`. By default, this parameter does not appear in the `opentext.ini` file, which is equivalent to `redirectPost=TRUE`.

resultCountLookAhead

- **Description:**

  Specifies the number of extra search results to permission check, and if the end of the "unpermissioned" result set can be reached in that range it will display the exact count.

- **Syntax:**

  `resultCountLookAhead=225`

- **Values:**

  An integer between `0` and `225`. By default, users can see `225` search results, which is equivalent to `resultCountLookAhead=225`. For more information about search results, see *OpenText Content Server - Administering Search (LLESWBS-AGD)*.

  Note: Specifying a value for this parameter does not guarantee an exact count of search results will be available.

TrueFileName

- **Description:**

  Specifies, for non-Enterprise data sources, for example, Directory Walker, XML Activator, and Spider data sources only, whether the actual file name is used for the `Name` value of the search result, rather than the DCS extracted value. For example, the `Name` will display as `DAVNode.os`, instead of `public String fAlwaysMimeType public Lis...`.

- **Syntax:**

  `TrueFileName=TRUE`

- **Values:**

  `TRUE` or `FALSE`. By default, this parameter does not appear in the opentext.ini file, which is equivalent to `TrueFileName=TRUE`.

wantMultipleEnterprise

- **Description:**

  Specifies whether to allow Administrators to create more than one Enterprise Data Source.

- **Syntax:**

  `wantMultipleEnterprise=FALSE`

- **Values:**

  `TRUE` or `FALSE`. By default, this parameter does not appear in the opentext.ini file, which is equivalent to `wantMultipleEnterprise=FALSE`. To enable the creation of more than one Enterprise Data Source, specify `wantMultipleEnterprise=TRUE`.

7.3.54 [Security]

The `[Security]` section sets Content Server security options.

allowedNextURLPrefixes

- **Description:**

  This parameter is evaluated only if `checkNextURL=TRUE`. Its value is the name of any URL prefix that Content Server accepts as a valid value for the `prefix` portion of a `NextURL` value. (For the meaning of `prefix`, see “checkNextURL” on page 209.)

- **Syntax:**

  ```
  allowedNextURLPrefixes={'/prefix/','/another/prefix/'}
  ```

allowedNextURLSites

- **Description:**

  This parameter is evaluated only if `checkNextURL=TRUE`. Its values are the names of any binaries that are not specified by the “cgiDirectory” on page 208 parameter and that Content Server accepts as values for the `CGI-file` portion of a `NextURL` value. (For the meaning of `CGI-file`, see “checkNextURL” on page 209.)

- **Syntax:**

  ```
  allowedNextURLSites={'<binary1.exe>', '<binary2.exe>'}
  ```

Authentication

- **Description:**

  This is OpenText proprietary information.

cgiDirectory

- **Description:**

  This parameter is evaluated only if `checkNextURL=TRUE`. Its value is the name of the folder that contains the Content Server CGI and ISAPI binaries (by default the *<Content_Server_home>*`\cgi\` folder). The names of the files contained in the `cgiDirectory` are accepted as values for the `CGI-file` portion of a `NextURL` value. (For the meaning of `CGI-file`, see “checkNextURL” on page 209.)

- **Syntax:**

  ```
  cgiDirectory=cgi
  ```

- **Values:**

  The name of the folder that contains the CGI and ISAPI binaries (by default the *<Content_Server_home>*`\cgi\` folder). The default value is `cgi`.

CGIHosts

- **Description:**

  A list of hosts from which the server accepts client connections. These connections are made from the CGI program, which is called `cs` on Linux systems and `cs.exe` on Windows systems. Since the CGI program and the server must be on the same host, the default value is the IP address `127.0.0.1`, which is a special IP address used for the localhost.

  If the list is empty, the server will accept CGI connections from any IP address.

- **Syntax:**

  ```
  CGIHosts=127.0.0.1
  ```

- **Values:**

  The default value is `127.0.0.1`, which is a special IP address used for the localhost. In rare circumstances, some systems may not recognize that this special IP address refers to the localhost. If this occurs, replace this special IP address with the unique IP address or host name of the localhost.

checkNextURL

- **Description:**

  This parameter enables `NextURL` validation.

  Setting `checkNextURL=TRUE` protects the `nextURL` value from attackers who want to direct Content Server users to other sites. If this parameter is enabled, Content Server evaluates the “cgiDirectory” on page 208, “allowedNextURLPrefixes” on page 208, and “allowedNextURLSites” on page 208 parameters to determine whether the value of the `nextURL` URL extension is permitted.

  Tip: The `NextURL` value is delivered to your browser as part of a response to certain requests.

  Example: If you submit a request to add a Task List, the server responds with the URL for a page that allows you to name the Task List. The URL includes a `NextURL` value. The `NextURL` value is the next logical request (expressed as a URL) to complete the addition of a Task List to Content Server.

  For the purposes of `NextURL` validation, a Content Server URL has the following components:

  ```
  <protocol>://<server>/<prefix>/<CGI-file>?func=...
  ```

  Example: In the following URL, the `server` is `my-server`, the `prefix` is `contentmgmt`, and the `CGI-file` is `cs.exe`:

  ```
  http://my-server/contentmgmt/cs.exe?func=...
  ```

  If `checkNextURL=TRUE`, the values of the components are compared to the values of the following parameters to determine whether the `nextURL` value is permitted.

<*protocol*>
Not evaluated by NextURL validation

<*server*>
Not evaluated by NextURL validation

<*prefix*>
"allowedNextURLPrefixes" on page 208

<*CGI-file*>
"cgiDirectory" on page 208, "allowedNextURLSites" on page 208

Note: Anything after the CGI-file portion of the URL is not evaluated by NextURL validation.

- **Syntax:**

  ```
  checkNextURL=TRUE
  ```

- **Values:**

  TRUE or FALSE. The default value is FALSE.

directoryList

- **Description:**

  This is OpenText proprietary information.

hideContainerSize

This opentext.ini setting is not present in Content Server 16.2.0 and later. If enabled in previous versions, it prevents Content Server from displaying the number of items in a container. To do this in Content Server 16.2.0 and later, enable **Hide Number of Items** on the **Configure Container Options** page. For more information, see "Configuring Container Options" on page 22.

7.3.55 [Servers]

The [Servers] section pertains to Content Server Explorer module use only. In this section, the Administrator provides a directory path mapping where a primary server connects to one or more secondary servers for the purpose of allowing users to perform actions on items between servers. Examples of these actions include: open, copy, and delete.

Content Server Explorer provides a view similar to that of the Windows Explorer familiar to users of Windows operating systems. If a secondary server name is mapped in the opentext.ini file, all users can see the name of the secondary server in the tree view, and make subsequent entries open folders, sub-folders and items.

In the following example, remote_0 is the name of the Content Server secondary server. It is followed by the URL that links the primary server to the secondary server.

```
#server_0=remote_0|http://myNT/support/cs.exe"
```

7.3.56 [socketServer_logs]

Contains settings that affect the generation of Content Server Socket Server logs.

OpenText recommends that you modify the values in this section on the **Configure Log Settings** page, rather than by editing the `opentext.ini` file. For more information, see "Configuring Log Settings" on page 33.

logLevel

- **Description:**

  Enables or disables the generation of Socket Server logs by setting the level of logging. You can specify a level of `0` (no logging), or `2` (logging enabled).

- **Syntax:**

  ```
  logLevel=2
  ```

- **Values:**

  Either 0 or 2. The default value is `2`.

7.3.57 [sockserv]

The `[sockserv]` section contains proprietary OpenText information.

Important
OpenText recommends that you do not change any of the options in this section.

7.3.58 [Summarizer]

The `[Summarizer]` section of the `opentext.ini` file controls one aspect of the Document Conversion Service, DCS. This service converts documents from their native formats to HTML, or raw text, for viewing and indexing purposes. DCSs are managed by Admin servers. The conversion services managed by the DCS share the parameters in the `opentext.ini` file. These parameters control the behavior of the conversion services. The `[Summarizer]` section, as a part of the DCS, is enabled by default.

Content Server Summarizer works with Content Server's search features to provide automatically generated summaries for documents. If Summarizer is turned on, and your display options in Content Server are set to display summaries, Content Server displays document summaries on the **Search Result** page after you perform a search. Summarizer generates summaries by compiling sentences based on their location in the document, the surrounding structures in the document, and the statistical significance of the words in the sentences. These sentences are identified in conjunction with the word frequency file, which is a configuration file that identifies the statistical frequency of words drawn from a large body of documents.

Summarizer also generates the key phrases associated with a document. Key phrases are phrases from the document that are likely to be indicative of the content. By default, Summarizer designates five phrases as key phrases, based on several factors, including the repetition of the phrases within the document and the location. If the document does not contain five suitable key phrases, Summarizer generates as many as it can. Key phrases are also displayed on the **Search Result** page after you perform a search, provided your display options in Content Server are set to display key phrases and Summarizer is enabled.

Summarizer begins by tokenizing source files to determine which elements are words, abbreviations, and so on. After defining the elements in the source file, Summarizer determines which series of tokens are readable sentences. It also analyzes the structure of the source file to determine which regions are most likely to contain good summary data. Summarizer then scores sentences according to the importance of words in both the document and the word frequency file, and then generates the summary. If Summarizer cannot summarize a source file, because of its structure or the readability of its sentences, its summary consists of the first 10 words in the file. If the source file does not have any word tokens, Summarizer does not generate a summary or key phrases.

OpenText has designed and configured Summarizer for English documents, but you can adjust its configuration to summarize documents in other languages. If you want to customize Summarizer, consider the following implications:

- Summarizer has the ability to summarize Japanese, French, and German, but has not been tested with languages other than English.
- Summarizer accommodates most sentence-ending punctuation from languages other than English.
- Multibyte languages can be summarized. Tokenization is Unicode-based.
- Summaries for languages requiring dictionary-based tokenization may not be complete.

The `[Summarizer]` section of the `opentext.ini` file contains the following parameters:

Important

OpenText strongly recommends that you do not modify the values of these parameters.

- "SumAbbrevFile" on page 213
- "SumDefFile" on page 213
- "SumDocFreqFile" on page 214
- "SumStopWordFile" on page 214
- "SumTagFile" on page 214

In addition to these parameters, this page also contains information about the following DCS parameters. These parameters are required settings that are only used by DCS.

- "lib" on page 215
- "summary" on page 216
- "summaryhotwords" on page 216
- "summarysentences" on page 216
- "summarysize" on page 217
- "summarytitlesize" on page 217
- "x-maxcalls" on page 217
- "x-timeout" on page 218

SumAbbrevFile

- **Description:**

  Specifies the relative path and name of the abbreviation file that Summarizer uses to define common abbreviations and all three-letter combinations that are not words.

- **Values:**

  A path and file name, relative to the location of the DCS in your Content Server installation. By default, the abbreviation file is named `abbrev.eng` and is stored in the config directory of your Content Server installation.

SumDefFile

- **Description:**

  Specifies the relative path and name of the definition file that Summarizer uses to define its operation. The definition file contains five numbers, one number per line, each representing the following:

  - A score multiplier for sentences that are in the first 20 percent of a document. These sentences are probably introductory sentences and are likely to be good summary sentences.
  - A maximum number of word tokens allowed in a summary sentence. A word token is a combination of letters, numbers, dashes, and entity references. Summarizer marks sentences containing more word tokens than the maximum number as unreadable and does not use them as summary sentences.
  - A minimum number of word tokens allowed in a summary sentence. Summarizer marks sentences containing fewer word tokens than the minimum number as unreadable and does not use them as summary sentences.
  - A maximum ratio of non-word tokens to word tokens. If the actual ratio of non-word tokens to word tokens exceeds this number, Summarizer marks the sentence as unreadable and does not use it as a summary sentence.
  - The number of documents used to form the data for the statistical significance of words in the word frequency file.

- **Values:**

A path and file name, relative to the location of the DCS in your Content Server installation. By default, the definition file is named `summdef.eng` and is stored in the config directory of your Content Server installation.

SumDocFreqFile

- **Description:**

  Specifies the relative path and name of the word frequency file that contains the data necessary for Summarizer to calculate the statistical significance of words in documents. This file contains a list of words that occurred in more than 1,000 of the 1,371,876 documents that OpenText used to build the statistical background for Summarizer's default settings.

- **Values:**

  A path and file name, relative to the location of the DCS in your Content Server installation. By default, the word frequency file is named `docfreq.eng` and is stored in the config directory of your Content Server installation.

SumStopWordFile

- **Description:**

  Specifies the relative path and name of the stopword file that Summarizer uses to define a list of common stopwords. Stopwords are words that add no semantic value to a sentence. These words are typically functional words such as “a”, “and”, and “the”. By distinguishing stopwords from semantically important words, Summarizer identifies which words are more likely to contribute to the document's distinct meaning, increasing the accuracy of its summaries and key phrases.

- **Values:**

  A path and file name, relative to the location of the DCS in your Content Server installation. By default, the stopword file is named `stopword.eng` and is stored in the config directory of your Content Server installation.

SumTagFile

- **Description:**

  Specifies the relative path and name of the tag file that contains a list of markup tags that appear in documents. Examples of markup tags include HTML, XML, and SGML. Next to each tag is a number that specifies the tag's importance to Summarizer. The following table describes the meaning of each number.

  Table describing the range of tag significance settings:

Number	Description
0	Summarizer ignores these tags, but does not ignore the data enclosed in them. If a sentence begins before this tag, and has this tag within it, Summarizer does not break the sentence into two sentences. By default, unknown tags are marked with this number.
1	Summarizer ignores these tags, but does not ignore the data enclosed in them. If a sentence begins before this tag, and has this tag within it, Summarizer breaks the sentence into two sentences.
2	Summarizer ignores these tags and the data enclosed in them.
3	This value marks the data enclosed in these tags as abstract, or overview, sentences. Summarizer creates the summary by using sentences in the title, abstract, and conclusion, in that order, before any other sentence.
4	This value marks the data enclosed in these tags as concluding sentences. Summarizer creates the summary by using sentences in the title, abstract, and conclusion, in that order, before any other sentence.
5	This value marks the data enclosed in these tags as title sentences. Summarizer creates the summary by using sentences in the title, abstract, and conclusion, in that order, before any other sentence.

- **Values:**

  A path and file name, relative to the location of the DCS in your Content Server installation. By default, the tag file is named `tags.eng` and is stored in the config directory of your Content Server installation.

lib

- **Description:**

  Specifies the name of the *library* to be loaded by the DCS. A library is a list of operations associated with a conversion filter that the DCS reads to perform conversion.

  Modifying the value of this parameter may prevent the DCS from functioning, or from functioning properly.

Important
Do not modify the value of this parameter unless directed to do so by OpenText Customer Support.

- **Values:**

  The default value is `dcssum`.

summary

- **Description:**

  Specifies whether the DCS generates summaries of the documents that it converts to HTML. If the user sets the search display options to show summaries, Content Server displays these summaries with search results on the **Search Result** page.

- **Values:**

  `TRUE` or `FALSE`, where `TRUE` instructs the DCS to generate summaries. By default, the `summary` parameter is set to `TRUE` on the command line of each DCS.

  To set the `summary` parameter to `FALSE`, you must use *OpenText Content Server - Administering Search (LLESWBS-AGD)* rather than change the parameter in the `opentext.ini` file, since arguments set on the command line override the global parameters set in the `opentext.ini` file.

summaryhotwords

- **Description:**

  Specifies the number of hotwords that Summarizer uses to generate a document summary. Reducing this value may speed up summarization, but there are many other variables that also affect the speed of this process.

  Important
  OpenText strongly recommends that you not modify the value of this parameter.

- **Values:**

  An integer greater than, or equal to, one. The default value is `20`.

summarysentences

- **Description:**

  Specifies the number of sentences to generate in summaries.

- **Syntax:**

  ```
  summarysentences=5
  ```

- **Values:**

  An integer greater than, or equal to, one. By default, this parameter does not appear in the `[Summarizer]` section of the `opentext.ini` file, which is equivalent to `summarysentences=5`.

summarysize

- **Description:**

  Specifies the portion of the converted document, in bytes, used by Content Server to generate a summary. A lower value restricts the summary to the first <*n*> bytes of the document. Changing this value may also affect document conversion performance of larger documents.

  Important
  OpenText strongly recommends that you do not modify the value of this parameter.

- **Values:**

  Any integer greater than one. The default value is `256000` bytes.

summarytitlesize

- **Description:**

  Specifies the number of characters to display in search result titles for specific documents. These documents originate from data sources other than the Content Server Enterprise data source, such as Directory Walker or Spider data sources.

- **Syntax:**

  ```
  summarytitlesize=30
  ```

- **Values:**

  An integer. The default value is `30`.

x-maxcalls

- **Description:**

  Specifies the number of times a worker process is reused for processing documents. During document conversion, the DCS loads a worker process. The worker process loads the appropriate conversion filter and uses it to convert the document. To increase performance, the DCS reuses the worker process for multiple conversions. If the worker process encounters an error, the process is stopped before reaching the value specified in the `opentext.ini` file.

  Important
  OpenText strongly recommends that you do not modify the value of this parameter.

- **Values:**

  The default value is inherited from the `maxcalls` parameter of the `[DCSworker]` section of the `opentext.ini` file.

  Note: The `x-maxcalls` parameter is only functional when the conversion filter it modifies is managed by a worker process. For more information about configuring a worker process, see *OpenText Content Server - Administering Search (LLESWBS-AGD)*.

Specifying a value for `x-maxcalls` will override the value of `maxcalls` in the `[DCSworker]` section of the `opentext.ini` file.

x-timeout

- **Description:**

  Specifies the maximum number of seconds to wait before terminating a document conversion worker process. You configure this parameter when the default value specified in the `timeout` parameter is inappropriate. You configure the `timeout` parameter on the `opentext.ini` page for each conversion filter. For example, some conversion filters convert documents slower than other conversion filters. In this case, the `timeout` default value of 30 seconds may not be applicable, as the average conversion time is longer than this value. In this case, you can modify the `x-timeout` value to a higher and more appropriate value.

  Important
  OpenText strongly recommends that you do not modify the value of this parameter.

- **Values:**

  The default value is inherited from the `timeout` parameter of the `[DCSworker]` section of the `opentext.ini` file.

  Note: The `x-timeout` parameter is only functional when the conversion filter it modifies is managed by a worker process. For more information about configuring a worker process, see *OpenText Content Server - Administering Search (LLESWBS-AGD)*.

  Specifying a value for `x-timeout` will override the value of `timeout` in the `[DCSworker]` section of the `opentext.ini` file.

7.3.59 [Tabs]

The `[Tabs]` section contains OpenText proprietary information.

Important
OpenText recommends that you do not change any of the options in this section.

7.3.60 [thread_logs]

Contains settings that affect the generation of Content Server thread logs.

OpenText recommends that you modify the values in this section on the **Configure Log Settings** page, rather than by editing the `opentext.ini` file. For more information, see "Configuring Log Settings" on page 33.

logLevel

- **Description:**

  Sets the level of logging. You can specify a level of `0` (no logging), `1` (warning messages), `2` (info messages) or `3` (debug messages).

- **Syntax:**

  ```
  logLevel=3
  ```

- **Values:**

  A number from 0 to 3. The default value is `0`.

logPath

- **Description:**

  The file path where the thread logs are generated.

- **Syntax:**

  ```
  logPath=.\logs\thread_logs\
  ```

- **Values:**

  A file path that is relative to the <*Content_Server_home*> folder, or an absolute file path. The default value is `.\logs\thread_logs\`.

enableRollingLogs

- **Description:**

  Enables rolling log files.

- **Syntax:**

  ```
  enableRollingLogs=FALSE
  ```

- **Values:**

  `TRUE` or `FALSE`. The default value is `FALSE`.

maxBackupIndex

- **Description:**

  If `enableRollingLogs=TRUE`, the number of rolling log files to keep before overwriting the oldest existing log file.

- **Syntax:**

  `maxBackupIndex=5`
- **Values:**

  A number between `1` and `13`. The default value is `10`.

maxFileSize

- **Description:**

  If `enableRollingLogs=TRUE`, the maximum size of a log file in megabytes. When a log file reaches its `maxFileSize`, Content Server creates a new log file and starts writing to it.
- **Example:**

  `maxFileSize=50`
- **Values:**

  A positive integer. The default value is `50`.

enableCompression

- **Description:**

  If `enableRollingLogs=TRUE`, causes completed log files to be compressed.
- **Syntax:**

  `enableCompression=FALSE`
- **Values:**

  `TRUE` or `FALSE`. The default value is `FALSE`.

enableBuffering

- **Description:**

  Buffer log file output in memory before writing to the log file, to enable faster performance at the cost of some risk of output not being written to a log file.
- **Syntax:**

  `enableBuffering=FALSE`
- **Values:**

  `TRUE` or `FALSE`. The default value is `FALSE`.

bufferSize

- **Description:**

  If `enableBuffering=TRUE`, the size in KB of the memory buffer used to hold log file output.
- **Syntax:**

```
bufferSize=10
```

- **Values:**

  A positive integer. The default value is `10`.

elevatedLoggingUserNames

- **Description:**

  For requests associated with any of the Content Server user IDs listed as values of this setting, generate thread logs at level 3 (debug). This setting overrides the level specified by `logLevel`, but only for the IDs listed.

- **Syntax:**

  ```
  elevatedLoggingUserNames=user1,user2,user3
  ```

- **Values:**

  One or more Content Server user IDs. If more than one user ID is listed, separate the user IDs with commas.

7.3.61 [timing_logs]

Contains settings that affect the generation of Content Server Summary Timing logs.

OpenText recommends that you modify the values in this section on the **Configure Log Settings** page, rather than by editing the `opentext.ini` file. For more information, see "Configuring Log Settings" on page 33.

logLevel

- **Description:**

  Sets the level of logging. You can specify a level of `0` (no logging), `1` (warning messages), `2` (info messages) or `3` (debug messages).

- **Syntax:**

  ```
  logLevel=3
  ```

- **Values:**

  A number from 0 to 3. The default value is `0`.

logPath

- **Description:**

  The file path where the timing logs are generated.

- **Syntax:**

  ```
  logPath=.\logs\timing_logs\
  ```

- **Values:**

  A file path that is relative to the <*Content_Server_home*> folder, or an absolute file path. The default value is `.\logs\timing_logs\`.

enableRollingLogs

- **Description:**

  Enables rolling log files.

- **Syntax:**

  `enableRollingLogs=FALSE`

- **Values:**

  `TRUE` or `FALSE`. The default value is `FALSE`.

maxBackupIndex

- **Description:**

  If `enableRollingLogs=TRUE`, the number of rolling log files to keep before overwriting the oldest existing log file.

- **Syntax:**

  `maxBackupIndex=5`

- **Values:**

  A number between `1` and `13`. The default value is `10`.

maxFileSize

- **Description:**

  If `enableRollingLogs=TRUE`, sets the maximum size of a log file in megabytes. When a log file reaches its `maxFileSize`, Content Server creates a new log file and starts writing to it.

- **Example:**

  `maxFileSize=50`

- **Values:**

  A positive integer. The default value is `50`.

enableCompression

- **Description:**

  If `enableRollingLogs=TRUE`, causes completed log files to be compressed.

- **Syntax:**

  `enableCompression=FALSE`

- **Values:**

  `TRUE` or `FALSE`. The default value is `FALSE`.

enableBuffering

- **Description:**

  Buffer log file output in memory before writing to the log file, to enable faster performance at the cost of some risk of output not being written to a log file.
- **Syntax:**

  `enableBuffering=FALSE`
- **Values:**

  `TRUE` or `FALSE`. The default value is `FALSE`.

bufferSize

- **Description:**

  If `enableBuffering=TRUE`, the size in KB of the memory buffer used to hold log file output.
- **Syntax:**

  `bufferSize=10`
- **Values:**

  A positive integer. The default value is `10`.

7.3.62 [trace_logs]

Contains settings that affect the generation of Content Server trace log files.

OpenText recommends that you modify the values in this section on the **Configure Log Settings** page, rather than by editing the `opentext.ini` file. For more information, see “Configuring Log Settings” on page 33.

enableTraceLogs

- **Description:**

  Enables the generation of trace log files.
- **Syntax:**

  `enableTraceLogs=true`
- **Values:**

  `TRUE` or `FALSE`. The default value is `TRUE`.

DeleteOlderLogFiles

- **Description:**

  Enables the deletion of the oldest trace log files if the quantity of trace log files in the folder exceeds a certain number.

- **Syntax:**

  `DeleteOlderLogFiles=TRUE`

- **Values:**

  `TRUE` or `FALSE`. The default value is `FALSE`.

logPath

- **Description:**

  The file path where the trace logs are generated.

- **Syntax:**

  `logPath=.\logs\trace_logs\`

- **Values:**

  A file path that is relative to the *<Content_Server_home>* folder, or an absolute file path. The default value is `.\logs\trace_logs\`.

NumberOfLogsToDeleteWhenOverLimit

- **Description:**

  If `DeleteOlderLogFiles=TRUE`, the number of log files to delete when the number of trace logs in the folder is greater than the value of `numberOfLogsToKeep`.

- **Syntax:**

  `NumberOfLogsToDeleteWhenOverLimit=50`

- **Values:**

  A positive integer. The default value is `50`.

numberOfLogsToKeep

- **Description:**

  The number of trace log files to retain in the log folder. When this number is exceeded, Content Server deletes the oldest trace log files. The number of trace files that Content Server deletes is the value of `NumberOfLogsToDeleteWhenOverLimit`.

- **Syntax:**

  `numberOfLogsToKeep=1000`

- **Values:**

  A positive integer. The default value is `1000`.

7.3.63 [unix_lang]

The `[unix_lang]` section, which is applicable to Linux only, contains system-specific information about the Content Server host's `locale`. For more information on `locale` functions and attributes, ask your system administrator.

LL_LC_ALL

- **Description:**

  Default language that the system uses for input and output. This corresponds to the `LANG` argument of the `locale` command. Leave this value set to the default.

- **Syntax:**

  ```
  LL_LC_ALL=C
  ```

- **Values:**

  Values are platform dependent. The default value, `C`, works on all platforms. This corresponds to the ANSI C 7-bit standard.

NLS_LANG

- **Description:**

  Specifies Oracle's internal `NLS_LANG` setting.

- **Values:**

  Operating-system dependent. As an example, a US-English Solaris machine uses `american_america.us7ascii` by default. Consult your Oracle documentation to determine an appropriate value for your installation.

NLS_SORT

- **Description:**

  Oracle client environment variable that determines how search results returned from the database are ordered.

- **Syntax:**

  ```
  NLS_SORT=binary
  ```

- **Values:**

  Any valid Oracle sort method. The default value is `binary`.

7.3.64 [UserSetting]

The `[UserSetting]` section controls the color settings of the Content Server user interface and Content Server user name display throughout the interface.

Color settings pertain to the color scheme seen on most Content Server pages. In general, most pages present data in rows and columns. Content Server users modify their default colors for column headers and rows by accessing the **Tools** menu.

User name displays are formats that identify how names appear in Content Server. The Administrator modifies name formats by making changes on the **Configure User Name Display** page of the Content Server Administration page.

This page contains information about the following parameters:

- "RowColorOptions" on page 226
- "ColumnHeaderColorOptions" on page 226
- "Row1Color" on page 227
- "Row2Color" on page 227
- "ColumnHeaderColor" on page 227
- "UserNameAppendID" on page 227

RowColorOptions

Important
The following information applies only to Content Server 16.2.1 and earlier. The `RowColorOptions` setting is deprecated in Content Server 16.2.2 and later. In Content Server 16.2.2 and later, it has no effect. For information on setting row colors, see *OpenText Content Server - Get Started (LLESRT-UGD)*.

- **Description:**

  Provides the six hexadecimal color value options available for users to select for Row 1 and Row 2. Users can change the default row color by modifying **Settings** on the **Tools** menu.

- **Syntax:**

  ```
  RowColorOptions=#FFFFFF,#EEEEEE,#FFFFCC,#CCFFFF,#CCFFCC,#DDDDFF
  ```

- **Values:**

  A comma separated list of any valid Hexadecimal color values.

ColumnHeaderColorOptions

- **Description:**

  Provides the four hexadecimal color value options for users to select for the column headers that appear on most Content Server pages. Users can change the default header column color by modifying **Settings** on the **Tools** menu.

- **Syntax:**

  ```
  ColumnHeaderColorOptions=#CCCCCC,#A0B8C8,#83D8A4,#CCCC99
  ```

- **Values:**

A comma separated list of any valid Hexadecimal color values.

Row1Color

- **Description:**

  Identifies a hexadecimal color value for Row 1. Any changes made to this field impacts only the local computer's INI settings, it does not impact any other user on the Content Server system.

- **Syntax:**

  ```
  Row1Color=#EEEEEE
  ```

- **Values:**

  Any valid Hexadecimal color value. The default color value is `#EEEEEE`.

Row2Color

- **Description:**

  Identifies a hexadecimal color value for Row 2. Any changes made to this field impacts only the local computer's INI settings, it does not impact any other user on the Content Server system.

- **Syntax:**

  ```
  Row2Color=#FFFFFF
  ```

- **Values:**

  Any valid Hexadecimal color value. The default color value is `#FFFFFF`.

ColumnHeaderColor

- **Description:**

  Identifies a hexadecimal color value for the column headers. Any changes made to this field impacts only the local computer's INI settings, it does not impact any other user on the Content Server system.

- **Syntax:**

  ```
  ColumnHeaderColor=#CCCCCC
  ```

- **Values:**

  Any valid Hexadecimal color value. The default color value is `#CCCCCC`.

UserNameAppendID

- **Description:**

  A format that allows the Content Server Log-in ID to append to the name display throughout Content Server. The `UserNameAppendID` setting can be changed only by the Administrator on the **Configure User Name Display** page of the administration interface.

- **Syntax:**

  ```
  UserNameAppendID=0
  ```

- **Values:**

  0 or 1. The default value is 0, or false, which means the Content Server Log-in ID will not append to the display name. The other valid value is 1, or true, which means the Content Server Log-in ID will append to the display name.

  An example of each would be:

  - If UserNameAppendID=0, the name display format is: John Q Public.
  - If UserNameAppendID=1, the name display format is: John Q Public (JQPublic).

7.3.65 [ViewableMimeTypes]

- **Description:**

  The [ViewableMimeTypes] section lists the MIME types of documents for which the Open operation should be treated like a Fetch. Content Server passes the document directly to the web browser without first trying to convert it to HTML for display.

- **Values:**

  The following is an example of the [ViewableMimeTypes] section in the opentext.ini file:

  ```
  MimeType_1=image/gif
  MimeType_2=image/jpeg
  MimeType_3=text/html
  MimeType_4=text/plain
  MimeType_5=application/pdf
  MimeType_6=application/x-zip-compressed
  MimeType_7=text/xml
  MimeType_8=message/rfc822
  MimeType_9=application/x-macbinary
  MimeType_10=image/pjpeg
  ```

7.3.66 [Workflow]

The [Workflow] section includes settings that control Workflow behavior.

ExcludedNodeSubTypes

- **Description:**

  Controls which items are excluded from the item reference attribute.

- **Syntax:**

  ```
  ExcludedNodeSubTypes={731,732,900,901,902,903,904,905,906,919,920}
  ```

- **Values:**

The node type ID of the items you want to exclude from the item reference attribute. The node type IDs that you specify for this parameter must be contained in braces, and each node type ID must be separated by a comma.

For example, the setting `ExcludedNodeSubTypes={141,142}` excludes the Enterprise Workspace, which is node type ID 141, and the Personal Workspace, which is node type ID 142, from the list of items that can be stored in an item reference attribute.

IHLogging

- **Description:**

  Controls Item Handler step logging.

- **Syntax:**

  `IHLogging={1}`

- **Values:**

  - **0**

    Disables Item Handler logging with time stamps.

  - **1**

    Enables Item Handler logging.

  - **11**

    Enables Item Handler logging with time stamps.

7.3.67 [XML]

The `[XML]` section contains the configuration settings for XML Export. By default, this section appears in the `opentext.ini` file when Content Server is installed. Please consult with OpenText Customer Support before making modifications to this section.

This page contains information about the following parameters:

• “Encoding” on page 230 • “StyleSheetMimeType” on page 230	• “MaxNodesToExport” on page 230 • “FetchSize” on page 230	• “UnencodedMimetype” on page 231

Note: An additional parameter, `LogPath`, can be added to the `[XML]` section to route the logging of XML import and export activity to its own directory. By default, XML log files are stored alongside other Content Server log files. For more information, see “Logpath” on page 156. If your Content Server system uses XML import and export extensively, you can add the line `LogPath=`*`<full_directory_path>`* to the `[XML]` section, where *<full_directory_path>* is the directory path that you specify.

Please consult with OpenText Customer Support before making this or any other modification to this section.

Encoding

- **Description:**

  Sets the encoding attribute of the XML declaration. An example of an XML declaration is: `<?xml version="1.0" encoding="ISO-8859-1"?>`.

- **Syntax:**

  ```
  encoding=ISO-8859-1
  ```

- **Values:**

  The default value is ISO-8859-1.

StyleSheetMimeType

- **Description:**

  Sets the value of the type attribute on the link to the stylesheet that is embedded in the XML export. An example of a stylesheet declaration is: `<?xml-stylesheet type="text/xsl" href=".."?>`. Microsoft IE5 requires the value `text/xsl`, which is not a formally recognized MIME type.

- **Syntax:**

  ```
  StyleSheetMimeType=text/xsl
  ```

- **Values:**

  The default value is `text/xsl`.

MaxNodesToExport

- **Description:**

  Sets the upper limit on how many nodes can be exported in a single export request. Zero, or a negative number, specifies an unlimited number of nodes.

- **Syntax:**

  ```
  MaxNodesToExport=1000
  ```

- **Values:**

  The default value is `1000`.

FetchSize

- **Description:**

  Sets the chunk size at which nodes are exported and written to the browser.

- **Syntax:**

  ```
  FetchSize=20
  ```

- **Values:**

  The default value is `20`.

UnencodedMimetype

- **Description:**

  Specifies the MIME types that can be exported unencoded when the `content` input parameter of the `XMLExport` request contains the value `cdata` or `plain`. If you do not specify the MIME type, the `cdata` and `plain` values are ignored.

- **Syntax:**

  ```
  UnencodedMimetype_1=text/xml
  ```

- **Values:**

  Valid MIME types.

Chapter 8

Administering MIME Types and Icons

By default, Content Server recognizes approximately 100 MIME types. *MIME* stands for Multipurpose Internet Mail Extensions, which is a standard used to identify the formats of files. You can modify the list of MIME types that Content Server recognizes by editing the `<Content_Server_home>/config/mime.types` file. The MIME types in this file are the ones that appear in the **MIME Type** list on the **Specific** tab of a Document's **Properties** page.

Similarly, you can modify the list of icon-to-MIME-type mappings by editing the `Content_Server_home/config/mime.gifs` file.

For information about modifying other system-configuration files, see "Modifying System Configuration Files" on page 90.

8.1 Modifying the MIME Types List

When a file is uploaded to the Content Server database, Content Server uses a variety of methods to determine its MIME type.

- Content Server looks for information about the file's MIME type from the user's web browser.
- Content Server looks up the file's extension in the `mime.types` file to see if it is mapped to a MIME type in that file.
- Content Server attempts to identify the MIME type using the Document Conversion Service.

You can set the order of these methods on the **Configure MIME Type Detection** administration page. If the first action fails to determine the MIME type, the next action occurs. If none of the methods are successful, Content Server assigns the file the `application/octet-stream` MIME type.

In addition to assigning MIME types to uploaded documents, the `mime.types` file controls the MIME types displayed in the **MIME Type** list on the **Specific** Properties tab in Content Server. By default, the `mime.types` file contains approximately 100 MIME types.

Using a text editor, you can modify the `mime.types` file to add a MIME type, remove a MIME type, or map a new file extension to an existing MIME type.

The Mime Types list

The **Mime Types** list can be found in the `<Content_Server_home>/config/mime.types` file, and it can be modified using a text editor.

Example 8-1: An Example of a Mime Types List

```
# MIME type to file extension mapping file.
#
# This is a whitespace-separated values file where blank lines and
text
# following "#" is ignored.
#
# Each line is a separate entry with the following format:
# <mime type> <file extension> ...
application/activemessage
application/andrew-inset
application/applefile
application/atomicmail
application/dca-rft
application/dec-dx
application/mac-binhex40
application/macwriteii
application/msword     doc W6BN
application/vnd.ms-excel  xls xlb XLS5
application/powerpoint   ppt SLD3
```

A MIME type is added to the list in the following format:

`<mime_type> <file_extension1> <file_extension2>` `...`

Taking one example of a <*mime_type*> from the MIME Types list above: `application/msword`, the two associated <*file_extensions*> are: `doc` and `W6BN`. However, when adding a new MIME type, it is not necessary to map a file extension to the MIME type.

You can use the # character to append a comment to any entry. Everything after the # character is considered to be a comment and is ignored by Content Server.

8.1.1 To Configure MIME Type Detection Rules

To configure MIME type detection rules:

1. In the **System Administration** section of the Content Server Administration page, click the **Configure MIME Type Detection** link.
2. On the **Configure MIME Type Detection** page, highlight any of the available MIME type detection methods and use the right arrow to move them to the **Selected Methods** field.
3. Once the methods you want used appear in the **Selected Methods** field, use the up and down arrows to place the methods in the order they should be used.
4. Click the **Save Changes** button.

8.1.2 To Modify the MIME Types List

To modify the MIME types list:

1. Open the *`<Content_Server_home>`*`/config/mime.types` file in a text editor.
2. To add a new MIME type to the `mime.types` file, add the MIME type on its own line in the format:

   `<mime_type> <file_extension1> <file_extension2>` `...`

   Note: It is not necessary to map a file extension to the MIME type.
3. To map a new file extension to an existing MIME type, append the extension to the MIME type's row, separating it from any other file extensions with a space.
4. To remove a MIME type entry, delete its line from the `mime.types` file.

   Tip: If you are not sure whether or not to permanently remove the MIME type, comment out the MIME type's line by inserting a `#` character at the beginning of the line instead of deleting it. This way, if you do need to use this MIME type in the future, you can remove the `#` character.
5. Save and close the `mime.types` file.
6. Restart Content Server and, if applicable, the web application server.

   If the updated list of MIME types does not immediately appear in the **MIME Types** list on the **Specific Info** page of a document, you may need to reload your web browser.

8.2 Modifying Icon-to-MIME type Mappings

The icons used to identify certain MIME types are controlled by the icon-to-MIME type mappings in the *`<Content_Server_home>`*`/config/mime.gifs` file. When a Content Server user adds a Document to the system, Content Server notes its MIME type and checks the `mime.gifs` file to see if a specific icon has been defined for the new file's MIME type. For example, if a user adds a Microsoft Word document to Content Server, a Microsoft Word icon appears next to it in Content Server, because the icon's GIF file has been mapped to the `application/msword` MIME type in the `mime.gifs` file.

If a document's MIME type is not specified in the `mime.gifs` file, Content Server uses a default document icon, .

You can edit the `mime.gifs` file to do any of the following:

- Associate a new or different icon file with an existing MIME type or types.
- Associate a new MIME type with an existing icon file.
- Associate a new MIME type with a new icon file.

Tip: You can use an image editor to create custom icons for use with the Documents you add to Content Server.

Creating a Custom Icon

If you want to create a custom icon for use by MIME types in Content Server, you should consider creating three different sizes of each custom icon:

- The default requirement is for a 16 × 16 pixel icon, , which you create in your `<Content_Server_home>/support/webdoc` directory.
- If a user chooses to make an item a Featured Item, Content Server displays a 32 × 32 pixel icon, which you create in your `<Content_Server_home>/support/webdoc` directory and your `<Content_Server_home>/support/mimetypeimages` directory.
- Content Server uses a 145 × 145 pixel icon on an item's **Overview** page. You create this icon in your `<Content_Server_home>/support/mimetypeimages` directory.

8.2.1 To Add a New Icon File

To add a new icon file:

1. Create an icon file in the General Internet Format image format, with the `.gif` file extension.
2. Create four copies of the new icon file, as follows
   - Create a 16 × 16 pixel icon in the `<Content_Server_home>/support/webdoc` directory.
   - Create a 32 × 32 pixel icon in the `<Content_Server_home>/support/webdoc` directory.
   - Create a 32 × 32 pixel icon in the `<Content_Server_home>/support/mimetypeimages` directory.
   - Create a 145 × 145 pixel icon in the `<Content_Server_home>/support/mimetypeimages` directory.
3. Map the new icon file to the desired MIME type(s). For more information, see “To Modify Icon-to-MIME Type Mappings” on page 237.

8.2.2 To Modify Icon-to-MIME Type Mappings

To modify icon-to-MIME type mappings:

1. Open the *<Content_Server_home>*/config/mime.gifs file in a text editor.
2. To associate a new MIME type with an existing icon file, type the new MIME type after the existing MIME types, separating them with spaces.
3. To associate a new icon file with new or existing MIME types, add an entry to the mime.gifs file in the following format:

   <gif_name> <file_name> <mime_type1> <mime_type2> ...
4. You can use the # character to append a comment to an icon mapping entry. Everything after the # character is considered to be a comment and is ignored by Content Server.
5. Make sure that any MIME type that you reference in the mime.gifs file is listed in the *<Content_Server_home>*/config/mime.types file. For more information, see “Modifying the MIME Types List” on page 233.
6. Do not associate a MIME type with more than one icon file.
7. Save and close the mime.gifs file.
8. Restart Content Server and, if applicable, the web application server.

Tip: If a new icon does not immediately appear in Content Server, you may need to reload your web browser.

8.3 Associating MIME Types and Categories

You can associate any available MIME type with an existing Category. When a MIME type is associated with more than one Category, and users add objects of that MIME type, they are directed to a second page during the **Add Item** process where they can choose which Category they want applied to that item.

In order to allow users to choose a Category when they add an item, if the item they are adding is of a MIME type that has more than one Category associated with it, you must select the **Display categories on second Add Item page** check box on the **Administer Item Control** page. For more information about item control parameters, see “Administering Item Control“ on page 335.

8.3.1 To Associate a MIME Type with a Category

To associate a MIME type with a Category:

1. In the **System Administration** section of the Content Server Administration page, click the **Administer MIME Types and Categories** link.
2. On the **Administer MIME Types and Categories** page, click the **Add Category** icon, ➕, to add existing Categories in Content Server to the **Categories** list.
3. In the **MIME Types** list, highlight each MIME Type that you want to associate, highlight each Category with which you want the MIME Type associated, and then click the **Associate Category** icon, 🔗.
4. Click **Submit**.

Chapter 9

Managing the Servers in Content Server

Managing the servers in Content Server includes the following tasks:

- "Stopping and Starting the Servers" on page 239
- "Backing Up and Restoring Content Server" on page 242

9.1 Stopping and Starting the Servers

When you perform certain system administration tasks, you must restart Content Server for the changes to take effect.

In most cases, when a restart is necessary, Content Server displays the **Restart Content Server** page. This page includes a **Restart** button that allows you to restart Content Server automatically (and a **Continue** button that allows you to bypass the automatic restart). However, there may be times when you prefer to restart Content Server manually, and occasionally you may need to restart Content Server in the absence of the **Restart Content Server** page. You may also need to restart the Content Server Admin server or the Content Server Cluster Agent, which are not restarted automatically. At such times, you can follow the instructions in this section to restart any of the Content Server servers.

There are three servers referred to in this section: Content Server , the Admin server, and the Cluster Agent. If you keep the default settings during the Microsoft Windows installation of Content Server, your servers are given the following default names:

- **Content Server (OTCS)**: referred to in the help as *Content Server*.
- **Content Server Admin (OTCS)**: referred to in the help as the *Admin server*.
- **Content Server Cluster Agent (OTCS)**: referred to in the help as the *Cluster Agent*

9.1.1 Stopping and Starting the Servers under Windows

Stopping the servers under Windows

To stop a server under Windows:

1. Open Windows **Services**.
2. Stop one or more of the Content Server services:

   a. To stop the `Content Server (OTCS)` service, right-click its name, and then click **Stop**.

b. To stop the `Content Server Admin (OTCS)` service, right-click its name, and then click **Stop**.

c. To stop the `Content Server Cluster Agent (OTCS)` service, right-click its name, and then click **Stop**.

Starting the servers under Windows

To start the servers under Windows:

1. Open Windows **Services**.

2. Start one or more of the Content Server services:

    a. To start the `Content Server (OTCS)` service, right-click its name, and then click **Start**.

    b. To start the `Content Server Admin (OTCS)` service, right-click the name of the Admin server, and then click **Start**.

    c. To start the `Content Server Cluster Agent (OTCS)` service, right-click its name, and then click **Start**.

9.1.2 Stopping and Starting the Servers under Linux

Stopping the Servers under Linux

Stopping or starting the Content Server process under Linux also shuts down or starts the Admin server process.

To stop Content Server and the Admin server under Linux:

1. Log on to the Linux host with the user name that Content Server uses.

2. At the command prompt, change to the directory where Content Server is installed.

3. Type the following command, and then press **ENTER**:

    ```
    ./stop_llserver
    ```

    Tip: To start only the Content Server Admin server process, run `./stop_lladmin`

To stop the Cluster Agent under Linux:

1. Log on to the Linux host with the user name that Content Server uses.

2. At the command prompt, change to the directory where Content Server is installed.

3. Type the following command, and then press **ENTER**:

    ```
    ./stop_otclusteragent
    ```

Starting the Servers under Linux

To start Content Server and the Admin server under Linux:

1. Log on to the Linux host with the user name that Content Server uses.
2. At the command prompt, change to the directory where Content Server is installed, and then do one of the following:
   - To start Content Server and the Admin server, type the following command, and then press **ENTER**:

     ```
     ./start_llserver
     ```

   - To start only the Admin server, (on a secondary Content Server host, for example), type the following command, and then press **ENTER**:

     ```
     ./start_lladmin
     ```

To start the Cluster Agent under Linux:

1. Log on to the Linux host with the user name that Content Server uses.
2. At the command prompt, change to the directory where Content Server is installed.
3. Type the following command, and then press **ENTER**:

   ```
   ./start_otclusteragent
   ```

9.1.3 Setting the Servers to Start Automatically

By default, the Content Server setup program configures Content Server, the Admin server, and the Cluster Agent to start automatically. (If you have multiple instances of Content Server installed on a host machine, the setup program only starts one instance of the Cluster Agent.) OpenText recommends that you do not alter this setting because Content Server requires these servers to function correctly. However, there may be times, such as when you are troubleshooting a problem, that you do not want the servers to start automatically when the primary Content Server host machine is restarted. In such cases, you can temporarily set one or more of the servers to manual startup, but make sure that you reset them to automatic startup when you are done.

Note: Whenever you restart Content Server, remember to restart your web application server, if you use one in your Content Server environment.

The procedures for setting Content Server, the Admin server, and the Cluster Agent to start automatically or manually differ on Windows and on Linux.

To modify the startup settings of a server under Windows:

1. Open Windows **Services**.
2. Right-click the name of the server whose startup setting you want to modify, and then click **Properties**.

3. On the **Startup type** menu:

   - To set the server to manual startup, choose **Manual**, and then click **OK**.
   - To set the server to automatic startup, choose **Automatic**, and then click **OK**.

To modify the startup settings of a server under Linux:

1. Log on to Linux as `root`.
2. Add the full path of `start_llserver`, `start_lladmin` or `start_otclusteragent` to the boot script of the Linux computer running the servers. Each of these scripts is located in the *`<Content_Server_home>`* directory.

Note: If you do not have root privileges or are unsure about modifying the boot script, consult your Linux system administrator.

There are several other ways to set up the servers to start automatically on Linux operating systems.

9.2 Backing Up and Restoring Content Server

You should back up Content Server periodically to protect the data that resides in your Content Server deployment. In addition, OpenText recommends that you back up Content Server whenever you apply an Update, install, uninstall, or upgrade a module, or make any other significant changes to your Content Server deployment.

A Content Server backup set consists of the following items:

- the <*Content_Server_home*> folder
- the Content Server database
- the External File Store
- one or more Search Indexes
- any Content Server folders that exist outside of the <*Content_Server_home*> folder, for example, an `Upload` folder.

Note: If your Content Server deployment includes optional modules or integrated applications, you may need to include additional items in the backup set.

Stop the Content Server services before you take a backup, so that all of the Content Server components are in sync with each other. Backing up Content Server while the Content Server services are running can result in data inconsistencies. For example, the Content Server database could contain references to Content Server items that do not exist in the backup of the External File Store.

To back up Content Server:

1. Stop Content Server, the Admin server, and the Cluster Agent.

2. Back up the Content Server database using tools that are appropriate for your relational database management system.

3. Back up the Content Server Search Indexes by making a copy of the `...\index\<index_name>` folder and its subfolders.

   Example: To back up the Enterprise Search Index, copy the `...\index\Enterprise\` folder and all of its subfolders.

   Note: See *OpenText Content Server - Administering Search (LLESWBS-AGD)* for information on automating index backups.

4. Back up the <*Content_Server_home*> folder by copying the folder and its subfolders.

5. Back up any Content Server folders that exist outside of the <*Content_Server_home*> folder, such as the Content Server `Upload` folder.

To restore a Content Server backup set:

1. Stop Content Server, the Admin server, and the Cluster Agent.

2. Restore your Content Server database.

3. Restore the Content Server Search Indexes.

4. Restore the <*Content_Server_home*> folder.

5. Restore any Content Server folders that exist outside of the <*Content_Server_home*> folder.

6. Start Content Server, the Admin server, and the Cluster Agent.

9.3 Generating a Sample Autoconfig File

The Autoconfig process is a mechanism that allows a minimum essential configuration to be applied to Content Server the first time it is started. Autoconfig is used as an alternative to running the installer, typically when using VM or container deployment methods. The **Generate Sample autoconfig.xml** feature is intended to be used on a working reference system to create a skeleton XML file which becomes a model for subsequent deployments. Edit the XML file to provide the missing configuration settings, then place it in the `<OTHOME>/config` directory of a new Content Server instance before first startup.

9.3.1 To Generate a Sample autoconfig.xml File

To Generate a Sample autoconfig.xml File

1. In the **Server Configuration** section of the Content Server Administration page, click the **Generate Sample autoconfig.xml File** link.

2. On the **Generate Sample autoconfig.xml File** page, choose the information from this Content Server system to include in the new `autoconfig.xml` file sections:

   - **Database** – **Omit**, or chose a database from the drop-down list
   - **Choose OTDS Type** – **Omit**, or chose an **Internal** or **External** installation of OpenText Directory Services from the drop-down list
   - **Enterprise Data Source** – select the check box to include an index of all the data that is stored in the Content Server database
   - **Metadata Language** – select the check box to quickly allow your users to add metadata tags in other languages
   - **OTDS** – **Omit**, or chose an **Internal** or **External** installation of OpenText Directory Services from the drop-down list
   - **Server Parameters** – select either or both check boxes to include the basic server and security parameters needed to get a minimum essential configuration of a new Content Server system running, or the default values

9.4 Using Custom Message Files

You can create custom message strings to add or replace error messages and labels of the standard UI by creating your own properties files in the `[OTHOME]/config/custom_strings` folder. This folder is not replaced when you apply a Content Server update. If this folder is not created it is just ignored as if no custom strings are present. The files in this folder need to be copied manually to each server of a clustered installation.

Note: The Smart UI and some standard UI browse table strings are not customizable by this method.

When Content Server starts, custom properties files corresponding to the enabled language packs are read and the xlats values within the files are applied to the server.

Each properties file must follow a strict naming convention, ending in `[language code].properties`. For example, [OTHome]/config/custom_strings/custom_fi_FI.properties

If keys are repeated in files of the same language code, the last definition remains.

Each custom string consists of a key-value pair, and follows the Java `.properties` file syntax. For details, see https://en.wikipedia.org/wiki/.properties

For example:

```
NEW_KEY.COMPANY = Acme
COLLECTIONS_COMMAND.CollectionsCommandAdministration = Collections
Command
```

The encoding of a `.properties` file is ISO-8859-1, also known as Latin-1. All non-Latin-1 characters must be entered by using Unicode escape characters, for example, `\u2013`.
The escape symbol `\` is required for the *leading space*, *trailing space*, `:`, `=`, and `#` characters.
Invalid lines are silently ignored.

9.5 Renaming a Content Server Host Computer

After you have installed and configured Content Server, OpenText recommends that you do not change the host name of a computer that runs Content Server. Renaming a Content Server computer is a complex operation that affects multiple Content Server components. If you must rename a Content Server computer, OpenText recommends that you obtain assistance from OpenText Professional Services before you proceed.

Chapter 10

Managing Licenses in Content Server

Content Server must be licensed before users without the `System administration rights` privilege can log on. You can apply a production, non-production, or temporary license to Content Server.

This chapter includes the following topics:

10.1 Licenses in Content Server

To license Content Server, you acquire a license file from OpenText, and then apply that license in OpenText Directory Services. Content Server licenses are tied to a *system fingerprint* that is generated from information in your Content Server database. The information is encrypted and hashed so that it not human-readable. A single license file is sufficient to license numerous Content Server instances that connect to the same database.

Certain Content Server modules also require licenses. Modules that require licenses appear on the **Manage Licenses** page, in the **Module License(s) Overview** section.

The following is a partial list of OpenText products that require a license. Please check the OpenText My Support (https://knowledge.opentext.com) site for a complete list.

- Content Server
- WebReports
- Object Importer / Object Exporter
- Archive Center

Important
Every OpenText product that requires a license, must have a license created for it in OTDS.

Most OpenText products will create a partial license in OTDS, provided you installed OTDS *prior to* the installation of either Content Server or its modules that require a license.

This is a requirement because Content Server, and its modules, have specific requirements regarding the name of the license that it will use. If you create a license in OTDS, as opposed to completing a partially created license, you will need to ensure that you use the correct name for that license.

Content Server has a requirement that its **License Key Name** field begins with “Content_Server”. For example, you can have the following as license key names that Content Server will recognize:

- Content_Server
- Content_Server 16.x.x Temporary
- Content_Server 16.2.0 Production

10.1.1 Obtaining a Content Server License

When you purchase Content Server or a Content Server optional module that requires licensing, you are provided with a link to download the installation software and a logon for the product activation site (http://productactivation.opentext.com/ContentServer). You use this logon to obtain your license file. For detailed steps, see “License Management” on page 252.

Types of License

The type of license that you have can be viewed in the **License Type** field on the **Manage Licenses** administrative page. Three types of license are available:

Production License
A Content Server production license enables full functionality for a specified number of licensed users. A production license is associated with a specific version of Content Server.

Temporary License
A temporary Content Server license enables all of the same functionality that a production license enables, but has an expiration date. The expiration date is always a specific date; it does not vary according to when you apply the temporary license.

Non-production License
A non-production license enables all of the same functionality that a production license enables, but is issued for use in any Content Server environment that is used to support a production environment. For example, you could apply a non-production license to a development environment or a User Acceptance Testing environment.

10.1.2 License Statuses

You can view the status of your Content Server license on the **Manage Licenses** administrative page. A Content Server license status can be:

Valid

A *valid* license status indicates that Content Server is licensed for use by a specified number of users.

Invalid

An *invalid* license status indicates an irregularity in your Content Server license:

- **Invalid Version**

  Your license applies to a different version of Content Server than the one that you are running

- **Invalid Fingerprint**

  Changes in your Content Server environment have caused your system fingerprint to change, so that it does not match the fingerprint in your Content Server license file.

- **Expired**

  The current date is after the Expiration Date specified in your temporary Content Server license. When its temporary license expires, Content Server operates in "Administrative Mode" on page 250.

- **Exceeded Users**

  The number of users in your Content Server environment is higher than the value of **Licensed Users** in your Content Server license.

  > **Tip:** If your license status is **Exceeded Users**, Content Server functionality is not affected and no users are locked out.

- **Invalid**

  Your Content Server license is invalid for a reason other than the ones listed above.

Unlicensed

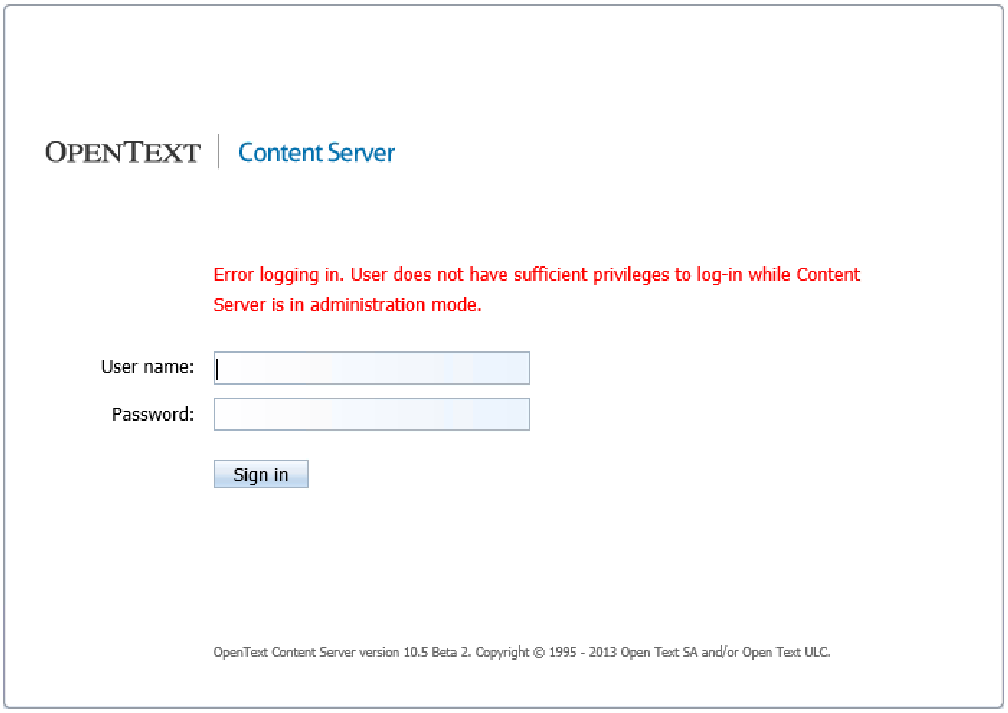
You have not applied a Content Server license to your Content Server installation. When Content Server is unlicensed, it operates in "Administrative Mode" on page 250.

10.1.3 Administrative Mode

Content Server operates in administrative mode when:

- its temporary license has expired
- it is unlicensed
- its license is invalid. The only exception to this case occurs in the event that the license is invalid due to “Exceeded Users”.

When Content Server is in administrative mode, only users with the `System administration rights` privilege can log on. Regular users cannot log on to Content Server. If a user without System administration rights attempts to log onto Content Server when it is in administrative mode, the following message appears:



Error logging in. User does not have sufficient privileges to log-in while Content Server is in administration mode.

User name:

Password:

OpenText Content Server version 10.5 Beta 2. Copyright © 1995 - 2013 Open Text SA and/or Open Text ULC.

To make Content Server exit administrative mode, apply a valid license.

10.2 Managing Content Server Licenses

There are four tabs on the **Manage Licenses** administration page:

- **License Overview**: you can view the status of your license(s), as well as view details for each license. For more information, see "Content Server License Overview" on page 251.
- **License Management**: you can view the Content Server System Fingerprint, access the OpenText product activation website, and access Directory Services apply a license file and manage your OpenText licenses. For more information, see "License Management" on page 252.
- **System Fingerprint**: you can view the Content Server System Fingerprint. For more information, see "System Fingerprint" on page 253.
- **License Report**: you can generate reports about your OpenText licenses. For more information, see "License Report" on page 253.

10.2.1 Content Server License Overview

The **Content Server License Overview** summarizes the features of your Content Server license:

Status
For information on license statuses, see "License Statuses" on page 249.

Product Name
The product licensed by this OpenText license: OpenText Content Server.

Licensed Version
The version of the product licensed by this OpenText license.

License Type
For information on License Types, see "Types of License" on page 248.

Company Name
The name of the company that the license is issued to.

Expiration Date
If your license type is `Temporary License`, an expiration date appears.

Licensed Users
Maximum number of users supported by this OpenText license. This field is only displayed for Content Server modules.

Active Users
Number of users that currently exist in Content Server.

The **Module License(s) Overview** summarizes the modules that are licensed by your Content Server license.

Tip: Not all modules require licenses.

10.2.2 License Management

On the **License Management** page, you can access:

- the OpenText Product Activation site to acquire a license
- OpenText Directory Services to apply a license file

To obtain a license file:

1. On the Content Server admin page, under **Server Configuration**, click **Manage Licenses**.

2. On the **Manage Licenses** page, select the **License Management** tab.

3. On the **License Management** page, a System Fingerprint appears that uniquely identifies your Content Server installation. Copy the System Fingerprint so that you can use it to generate a license file for Content Server or for a Content Server optional module.

4. Click the product activation link to open the OpenText product activation website. Logon to the website using the userid and password provided to you when you purchased your OpenText product.

   The OpenText product activation website is located at http://productactivation.opentext.com/ContentServer.

5. If you have more than one Content Server environment, select the environment to which you will be applying the license.

   Tip: Only one license is required for multiple instances of Content Server that connect to the same database.

6. Select the appropriate product and license file type, and use the System Fingerprint you copied in Step 3 to generate a license file.

To apply a license file:

1. On the Content Server admin page, under **Server Configuration**, click **Manage Licenses**.

2. On the **Manage Licenses** page, select the **License Management** tab.

3. On the **License Management** page, click the **Manage Licenses** button.

4. OpenText Directory Services **License Keys** page will open in a new tab. If you are prompted to sign in to OTDS, sign in with your user name and password.

5. Provided you installed OTDS before you installed Content Server, a partially created license stub has been created for you to complete. Follow the instructions in the *OpenText Directory Services - Installation and Administration Guide (OTDS-IWC)* to create your license in OTDS.

6. If you have applied or changed a license to Content Server, or to any Content Server module, you must restart the Content Server admin servers. For more information, see "Stopping and Starting the Servers" on page 239.

10.2.3 System Fingerprint

A system fingerprint uniquely identifies your Content Server deployment, using pieces of information from your Content Server database. The information is encrypted and hashed so that it is not readable, even by OpenText. The system fingerprint is the same for every instance of Content Server in your deployment, provided each instance connects to the same Content Server database.

Invalid System Fingerprint

In the unlikely event that changes in your database cause your system fingerprint to become invalid, your license status appears as `Invalid Fingerprint` on your **Content Server License Overview**.

Having an invalid system fingerprint has no effect on your deployment. Your users can continue to access Content Server normally. The system does not enter administrative mode. However, if you see that your license status is `Invalid Fingerprint`, OpenText recommends that you contact Technical Support for assistance.

10.2.4 License Report

The **License Report** page displays detailed information on your Content Server license, including your End User Code, System Unique Identifier (SUID), and System Fingerprint. To generate an XML copy of this report, click **Generate Report**.

Part 3

System Administration

Chapter 11

Managing UI Languages

The multilingual feature allows you to translate all user interface elements – dialog boxes, status bars, toolbars, hyperlinks, menus, tabs, labels of drop-down menus, text fields, and online help – into a localized language on one Content Server instance.

11.1 Creating, Installing and Upgrading Language Packs

A *Localization Kit* is available on OpenText My Support (https://knowledge.opentext.com). Before you can configure languages, you must create a new language pack and install it on the computer where Content Server is installed.

When a new instance of Content Server is installed, English is always the default language. French, German, Japanese and Dutch language packs are included in the Content Server installation. If you intend using one of these five languages, it is not necessary to create a new Localization Kit.

Important
OpenText strongly recommends that you delete and recreate the User Help Data Source Folder and the Admin Help Data Source Folder whenever you add or remove language packs, or when the system default locale is modified. For more information, see *OpenText Content Server - Administering Search (LLESWBS-AGD)*.

Installing Language Packs

Once you have the language pack you want to install, and depending on whether this is a Content Server system language pack or a Content Server module language pack, you need to do one of two things:

1. If you are installing a Content Server system language pack, you need to unzip the language pack to the root Content Server installation directory.

   For example, if you installed Content Server to the `C:\OPENTEXT` directory, unzip the language pack you have downloaded, or created, to the `C:\OPENTEXT` directory. The language pack will be unzipped to `C:\OPENTEXT\langpkgstaging`.

2. If you are installing a Content Server module language pack, you need to unzip the language pack to the `C:\<Content_Server_home>\langpkgstaging\module` directory, where `C:\<Content_Server_home>` is the location of your Content Server installation.

Note: When you install a language pack, if settings already exist in the `opentext.ini` file, and the value of the setting is not empty, the values will be overwritten with the settings in the language pack you install.

Once a language is installed, the language code will appear in alphabetical order under the **Languages** section on the **Installed Language Packs** page. Content Server, and each Content Server module, will show all available languages; if a language is not installed for a particular module, a “No languages installed” message is listed. For more information about language names and codes, see “Configuring Languages” on page 261.

You can specify a different user display name format for each language. The display name for users can be their Log-in ID, or their first name, last name, and middle initial. You can also choose to append the users' Log-in IDs to the format you choose. For more information, see “Configuring User Settings” on page 427.

When you install a language, it may be necessary to update the way dates and times appear to match the standard of that language. For example, the default date format is set to appear as *month/day/year*, but you may want to set it to a *year/month/day* format. You can specify the format for each installed language. For more information, see “Setting Date and Time Formats” on page 30.

Upgrading Language Packs

Content Server language packs can be upgraded. OpenText releases updated language packs, for each of the languages shipped with Content Server, with each Content Server update.

There are two ways that you can upgrade your language packs:

1. When you upgrade Content Server to the latest patch or service pack, you can also download the latest language packs.
2. You can also download the latest language packs from OpenText My Support (https://knowledge.opentext.com) and install those updated language packs on your Content Server system.

Once you have the updated language pack you want to install, you need to unzip it to the proper directory:

1. If you are installing an updated language pack to the Content Server system, unzip the updated language pack to the root Content Server installation directory.

   For example, if you installed Content Server to the `C:\OPENTEXT` directory, unzip the updated language pack you have downloaded to the `C:\OPENTEXT` directory. The updated language pack will be unzipped to `C:\OPENTEXT\langpkgstaging`.
2. If you are installing an updated language pack to a Content Server module, unzip the updated language pack to the `C:\`*`<Content_Server_home>`*`\langpkgstaging\module` directory, where `C:\`*`<Content_Server_home>`* is the location of your Content Server installation.

Important

Because customers can download and install full language packs with each Content Server update, each full language pack will overwrite the corresponding, existing language pack, provided the version of the language pack you are installing is *equal to or greater* than the currently installed language pack.

Content Server will generate an error message if the updated language pack you are attempting to install is an older version than the currently installed language pack.

For more information, see "To Update a Language Pack for Content Server" on page 260.

Disabling Language Packs

Language packs cannot be uninstalled, but they can be disabled. For more information on how to disable a language pack, see "Configuring Languages" on page 261.

11.1.1 To Install a Language Pack for Content Server

To install a language pack for Content Server:

1. Download the language pack that you want to install and extract it to the *<Content_Server_home>* folder, so that it adds files to the `C:\`*`<Content_Server_home>`*`\langpkgstaging\module` location (where `C:\`*`<Content_Server_home>`* is the location of your Content Server installation).

   Note: Do not change the default name of the language pack.

2. On the **Content Server Administration** page, in the **Languages** section, click **Install Language Packs**.
3. On the **Install Language Packs** page, in the **Installable Content Server Language Packs** section, enable each language pack that you want to install, and then click **Install**.
4. When the **Installation Summary** page appears, restart Content Server.
5. Click **Continue**.

Note: After you install a language pack, you must enable it in the **Configure Languages** section in order to apply the new language to the entire system. For information about enabling language packs, see "Configuring Languages" on page 261.

11.1.2 To Install a Language Pack for a Content Server Module

To install a language pack for a Content Server module:

1. Download the module language pack that you want to install and extract it to the <*Content_Server_home*> folder, so that it adds files to the `C:\<Content_Server_home>\langpkgstaging\module` location (where `C:\<Content_Server_home>` is the location of your Content Server installation).

   Note: Do not change the default name of the module language pack.

2. On the **Content Server Administration** page, in the **Languages** section, click **Install Language Packs**.
3. On the **Install Language Packs** page, in the **Installable Module Language Packs** section, enable each module language pack that you want to install, and then click **Install**.
4. When the **Installation Summary** page appears, restart Content Server.
5. Click **Continue**.

11.1.3 To Update a Language Pack for Content Server

To update a language pack for Content Server:

1. Download the updated language pack that you want to install, and extract it to the <*Content_Server_home*> folder.

   Note: Do not change the default name of the updated language pack.

2. On the **Content Server Administration** page, in the **Languages** section, click **Install Language Packs**.
3. On the **Install Language Packs** page, in the **Installable Content Server Language Packs** section, enable each language pack update that you want to update, and then click the **Install** button.
4. When the **Installation Summary** page appears, restart Content Server.
5. Click **Continue**.

11.1.4 To Update a Language Pack for a Content Server Module

To update a language pack for a Content Server module:

1. Download the updated language pack that you want to install, then and extract it to the <*Content_Server_home*> folder, so that it adds files to the`C:\<Content_Server_home>\langpkgstaging\module` location (where `C:\<Content_Server_home>` is the location of your Content Server installation).

   Note: Do not change the default name of the updated language pack.

2. On the **Content Server Administration** page, in the **Languages** section, click **Install Language Packs**.
3. On the **Install Language Packs** page, in the **Installable Module Language Packs** section, enable each language pack that you want to upgrade, and then click **Install**.
4. When the **Installation Summary** page appears, restart Content Server.
5. Click **Continue**.

11.1.5 To View Installed Language Packs

To view installed language packs:

- Click the **View Installed Language Packs** link in the **Languages** section on the Content Server Administration page.

11.2 Configuring Languages

Once you install a language pack, you can use the Administration page to enable, disable, and change the default system language. Users can see all languages that are enabled, and select which language they want Content Server to use when they log in. Users cannot see or select languages that are installed but not enabled.

Note: The current system default language cannot be disabled or removed. If you want to disable a language, you must first enable and specify a different language as the system default language.

Each language has a default language name, local language name, and associated language code. For example, the English language is listed as “English (United States)” for both language and local language, but it either name can be changed if necessary. The language code is a default value, and cannot be changed.

11.2.1 To Enable, Disable, and Change the Default System Language

To enable, disable, and change the default system language:

1. In the **Languages** section of the Content Server Administration page, click the **Configure Languages** link.
2. On the Configure Languages page, do any of the following:
    - To enable or disable a language, select or clear the **Enabled** check box beside the language.
    - To change the system default language, click the **System Default** radio button beside the language you want to specify as the default.
    - To edit the language name, click the **Edit** button, type a name for the language and the local language in the **Language** and **Language (Local)** fields, and then click the **Save** button.
3. Click the **OK** button.

Chapter 12

Working with Multilingual Metadata

The Multilingual Metadata functionality enables users to modify the names and descriptions of objects in Content Server using languages that you enable. The metadata is captured in audit trails and is searchable.

12.1 Configuring Multilingual Metadata

In order to allow users to add metadata tags in other languages, you must first add the language, then enable it. Once languages, other than the default, are enabled, the **Edit Multilingual Values** icon appears next to an object's **Name** and **Description** fields. Once a language is enabled, you can modify the default language name or specify it as the system default, which means when a user clicks the **Edit Multilingual Values** icon, the default metadata language appears first in the list if that user has not selected a preferred language.

Note: Even though the system default language *can* be specified, it is not recommended that you modify the system default. The system default language is normally assigned during the installation or upgrade process.

OpenText strongly recommends you delete and recreate the Help Data Source Folder and the Admin Help Data Source Folder whenever you add or remove language packs, or when the system default language is modified.

12.1.1 To Add a Metadata Language

To add a metadata language:

1. In the **Metadata** section of the Content Server Administration page, click the **Configure Multilingual Metadata** link.
2. On the **Configure Multilingual Metadata** page, select a language to add in the **Add New Metadata Language** list, and then click the **Add** button.

Note: After a metadata language is added, you must enable it.

OpenText strongly recommends you delete and recreate the Help Data Source Folder and the Admin Help Data Source Folder whenever you add or remove language packs, or when the system default language is modified.

12.1.2 To Configure Multilingual Metadata Parameters

To Configure Multilingual Metadata Parameters:

1. In the **Metadata** section of the Content Server Administration page, click the **Configure Multilingual Metadata** link.
2. Do any of the following:
   - To enable a language, select the **Enabled** check box for any language you want to enable.
   - To specify the language as the default language for Content Server, click the **System Default** button for the language.
   - To edit the language name, click the language's **Edit** icon, type a new language in the **Language** or **Language (Local)** fields, and then click **Save**.
   - To delete a language that has been added, click the language's **Delete** icon, and then click **Yes** in the confirmation window.
3. Click **OK**.

Chapter 13

Working with Memcache

Memcached processes are managed in the same manner as Content Server search processes. The memcached processes are registered with the admin servers through the **System Object Volume** page. Content Server will install three default memcached nodes:

- Memcached 1
- Memcached 2
- Memcached 3

To view these default memcached nodes, see "To View the Memcached Processes" on page 265.

13.1 To View the Memcached Processes

To view the memcached processes:

1. On the Content Server Administration page, under the **Search Administration** section, click **Open the System Object Volume**.
2. On the **Content Server System** page, click **Process Folder**.

13.2 To View the Memcached Statistics

To view the memcached statistics:

1. On the Content Server Administration page, under the **System Administration** section, click **Memcached Statistics**.
2. On the **Memcached Statistics** page you will see:

Memcached Statistic	Description
Status	The status for each cached process. Possible values include *Idle* and *Running*.
Name	The name of the cached process as a link. Click this link to see the details page for that process.
Host Name	The name of the host system on which this memcached process resides.
Port	The port number of the host system on which this memcached process listens.
Version	The version number of the server.

Memcached Statistic	**Description**
Get Hits	The number of successful “get” commands since startup.
Get Misses	The number of failed “get” commands since startup.
User Time	The number of user time seconds for this memcached process.
System Time	The number of system time seconds for this memcached process.
Number of Items	The number of items *currently* stored in this memcached server's cache.
Total Number of Items	The total number of items *ever* stored in this memcached server's cache. The count is increased by every new item stored in the cache.
Bytes	The number of bytes currently used for caching items on this memcached server. For the maximum allowed bytes, see “Maxbytes” below.
Open Connections	The number of open connections to this memcached server.
Total Connections	The total number of connections available on this memcached server.
Retrieval Requests	The number of retrieval requests sent to this memcached server.
Storage Requests	The number of storage requests sent to this memcached server.
Bytes Read	The total number of bytes received by this memcached server from the network.
Bytes Written	The total number of bytes sent by this memcached server to the network.
Maxbytes	The maximum configured cache size, in bytes, for this memcached server.

13.3 To View or Change the Properties of a Memcached Process

To view or change the properties of a memcached process:

1. On the Content Server Administration page, under the **System Administration** section, click **Memcached Statistics**.
2. On the **Memcached Statistics** page, under the **Name** column, click the name of the memcached process you want to view.
3. On the <*memcache_process_name*> properties page, click the **General** tab. Next, do any of the following:

   a. Optional If you want to change the name of the process, in the **Name** field, type the new name for the process.

   b. Optional In the **Description** field, type a description of the process.
4. Click **Update**.

13.4 To Start or Stop a Memcached Process

To start or stop a memcached process:

1. On the Content Server Administration page, under the **System Administration** section, click **Memcached Statistics**.
2. On the **Memcached Statistics** page, under the **Name** column, select the name of a memcached process you want to start or stop.
3. On the <*memcache_process_name*> properties page, click the **Specific** tab.
4. Optional Under the **Actions** section, if the process has been stopped, click the **Start** button. If the process is running, click the **Stop** button.
5. Click **Update**.

13.5 To Resynchronize a Memcached Process

To resynchronize a memcached process:

1. On the Content Server Administration page, under the **System Administration** section, click **Memcached Statistics**.
2. On the **Memcached Statistics** page, under the **Name** column, select the name of a memcached process you want to resynchronize.
3. On the <*memcache_process_name*> properties page, click the **Specific** tab.
4. Optional Under the **Actions** section, click **Resynchronize**.

5. On the **Content Server Process Resynchronization Results** page, read the information message, and then click **Continue**.

13.6 To Add a Memcached Process

To add a memcached process:

1. On the Content Server Administration page, under the **Search Administration** section, click the **Open the System Object Volume** link.
2. On the **Open the System Object Volume** page, click **Process Folder**.
3. On the **Process Folder** page, from the **Add Item** menu, select **Memcached Process**.
4. On the **Add: Memcached Process** page, in the **Name** field, enter a name for your new process.
5. Optional In the **Description** field, enter a description for your new process.
6. Optional In the **Host** field, you can optionally change the default host using the associated list.
7. In the **Port Number** field, enter an available port number for your new process. Once you have entered the port number, click the **Check port** link to be certain that this port number is available.
8. Optional In the **Memory Usage** field, change the default memory usage setting using the associated list.
9. Optional In the **Additional Command Line** field, enter any additional command line options to run with your new process.

Chapter 14

Configuring Rendering Settings

From the **Configure Rendering Settings** page, you can enable the **Use Versioned Resources** setting to minimize the need for users to refresh their browser caches after Content Server upgrades.

You can also set the *BASE HREF* value in an HTML page that includes a custom view. If no values are present in this page, default values in the HTTP request are used. The following settings are available:

- **Generate WebLingo Filename Comments**: Select this check box to add comments to every generated HTML page in Content Server to describe which WebLingo template file generated that page. This is mainly used for debugging.
- **Host to Replace**: a text field where you enter the host name of the URL that is used to load the page you are viewing. This value will be replaced by the value entered in the **Host** field.
- **Protocol**: a list from which you can select either *http* or *https*.
- **Host**: a text field which allows you to enter the hostname of the server to include in the BASE HREF URL.
- **Port**: a text field which allows you to enter the port of the web server used in the BASE HREF URL.
- **Default Encoding for Text Documents**: Content Server attempts to verify if a text document is UTF-8 encoded. If it is not UTF-8 encoded, Content Server delivers the encoding directive specified by this setting.

  Note: Text documents transmitted with HTTP send a *`charset`* parameter in the HTTP header to specify the character encoding of the document. The value specified in the **Default Encoding for Text Documents** field will become the value of the charset parameter. For example, if you set the **Default Encoding for Text Documents** parameter to `shift-jis`, the resulting line in the HTTP header would look like the following: `Content-Type: text/plain; charset=shift-jis`.

For information about how these settings appear in the `opentext.ini` file, see "[BaseHref]" on page 98.

14.1 To Configure Rendering Settings

To configure rendering settings

1. Click the **Configure Rendering Settings** link in the **System Administration** section on the Content Server Administration page.

2. Optional To add comments to describe which WebLingo template file generated a particular Content Server HTML page, select the **Generate WebLingo Filename Comments** check box.

3. Optional To minimize the need for browser refreshes after Content Server upgrades, select the **Use Versioned Resources** check box. This should ensure that new updates can deploy without your users needing to refresh their browser caches.

   Note: Not all proxy servers support caching of versioned resources.

4. Optional In the **Base Href Settings** section, do the following:

   a. In the **Host to Replace** field, type the name of the Host portion of the URL that will be replaced by the value entered in the **Host** field.

   b. In the **Protocol** field, select either *http* or *https* from the list.

   c. In the **Host** field, type the name of the host.

   d. In the **Port** field, type the port number.

5. In the **Default Encoding for Text Documents** field, type the Content-Type character set to use when text documents are not UTF-8 encoded.

Part 4

Database Administration

Chapter 15

Changing Your Content Server Database

A Content Server database is created as part of the Content Server installation. If you have a working Content Server database, you do not normally need to create a new one or switch to a different one. However, on occasion, you may wish to change your Content Server database.

For example, if you have been using Content Server with a test database and you now wish to move Content Server to production, or if you are restoring a database backup and you do not wish to overwrite your current database, you could create a new database. And if you are upgrading Content Server, changing your database is integral to the process: part of the upgrade process is to disconnect from a staging database created for your new Content Server version, connect to your existing production database, and then upgrade it.

Overall, the procedure of changing your Content Server database consists of:

Exporting OTDS data

This step only applies if the Content Server instance you are upgrading is using an internal installation of OTDS. If your Content Server instance is using CSDS, you need to migrate your Content Server users and CSDS sync sources.

Export OTDS data allows you to export your OTDS configuration and user data to an `LDIF` file. In the event that you need to change your Content Server database, an export of your OTDS data to an `LDIF` file allows you to import that data to OTDS after you change your Content Server database.

Exporting the OTDS data preserves all of the internal OTDS configuration, partitions, and user data associated with the OTDS database so that you can import that OTDS data to any Content Server installation that uses the same Content Server database.

Failure to perform an export of the OTDS data will result in the loss of that data following a Content Server database change or upgrade.

For information on the **Export OTDS data** option, see *OpenText Content Server - Administering OpenText Directory Services Integration Administration (LLESDSI-AGD)*.

"Deselecting Your Current Database" on page 274

You disconnect from your current Content Server database and, optionally, drop the data source folder that contains your Search index.

> **Tip:** After you deselect your current Content Server database, you can no longer access this online help. To retain access to these instructions, keep this window open, print a copy of this section before you disconnect, or view the Content Server Admin Help on OpenText My Support.

"Adding and Connecting to a new Content Server Database" on page 276 **or** "Connecting to an Existing Database" on page 287

If you are creating a new database, you log onto your RDBMS, create a Content Server database and database user, and then create your Content Server database tables. The exact procedure depends on your RDBMS.

If the Content Server database already exists, you can connect to it by logging on as the Content Server database user. If the database contains the Content Server tables, it is ready to use. If it does not, you can create the Content Server database tables when you connect.

"Configuring Content Server After Changing Your Database" on page 294

After you switch to a different Content Server database, you will need to perform some or all of the following additional steps:

- Upgrade the database
- Configure Content Server to use OpenText Directory Services
- Install additional Content Server modules
- Configure one or more Admin servers
- License Content Server

Each of these tasks is looked at in greater detail in this section.

15.1 Deselecting Your Current Database

Before you can create a new Content Server database or connect to an existing one, you must disconnect from your current Content Server database.

When you deselect your current Content Server database, you are offered the choice of deleting or keeping the data sources that are associated with your current database. The default option is to delete the data sources, but if you think you might have any reason for keeping them, clear the **Delete** option. You can always delete the data sources later.

To deselect your current Content Server database:

1. On the Content Server Administration page, in the **Database Administration** section, click **Change Current Database**.

2. The **Deselect Content Server Database** page appears. It displays information on your current Content Server database, and lists each data source that is associated with this database.

   a. Optional By default, **Delete** is enabled beside each data source, meaning the folder at the path in the **Index Location** column will be deleted when the new Content Server database is created. If you wish to retain the data source folder, clear the **Delete** check box.

b. Optional If your current Content Server deployment uses an Internal OTDS, click **Export OTDS data** to save your OTDS data to an `LDIF` file that you can use to restore users, groups and other OTDS data if you ever re-use the database that you are deselecting.

> **Important**
>
> If your Content Server deployment uses an Internal OTDS and you do not export your OTDS data when you deselect the database, the OTDS data cannot be recovered.

c. Click **Continue** to deselect your current Content Server database.

3. The **Restart Content Server** page appears. Click **Restart** to restart Content Server automatically, or click **Continue**, if you prefer to use operating system tools to restart Content Server.

> **Important**
>
> Before you connect to a different database:
>
> 1. Stop every Admin server.
> 2. Remove the `search.ini` and `otadmin.cfg` files from the `Content Server/config` folder of each Admin server to prevent orphaned processes from being carried to another database.
> 3. Start each Admin server.
>
> After you connect to the new database, resynchronize each Admin server to create new `search.ini` and `otadmin.cfg` files.

After you deselect your current database, the **Database Administration** page appears, and you can proceed with one of the following options:

Create New Database
Choose this option to create a new Content Server database, Content Server database user, and Content Server database tables. For more information, see "Adding and Connecting to a new Content Server Database" on page 276

Select Existing Database
Choose this option to connect to an existing Content Server database (that has Content Server database tables in it) as an existing Content Server database user. For more information, see "To Connect to an Existing Content Server Database" on page 291.

Create Tables in Existing Database
Choose this option to connect to a Content Server database that has no tables in it as an existing Content Server database user. For more information, see "To Connect to an Existing Empty Database" on page 287.

15.2 Adding and Connecting to a new Content Server Database

After you deselect your current database (see "Deselecting Your Current Database" on page 274), the **Database Administration** page appears, and you can create a new Content Server database.

Tips

- For recommendations on configuring your Content Server database, see *OpenText Content Server - Installation Guide (LLESCOR-IGD)*.
- When you create a Content Server database, you specify whether Content Server uses External Document Storage (file system storage) for its documents and other items. If you do not enable External Document Storage, Content Server stores all of its item in its database. For more information on storage options, see "Storage Providers and Storage Management" on page 383.

To begin creating a new Content Server database, click **Create New Database**. On the **Select RDBMS** page, enable the type of database that you wish to create, and then click **Continue**.

SAP HANA
To create a HANA database, see "Adding and Connecting to a New SAP HANA Database" on page 277.

Oracle Server
To create an Oracle database, see "Adding and Connecting to a New Oracle Database" on page 279.

Tip: If the option to create an Oracle database does not appear on the **Select RDBMS Type** page, ensure that you have installed Oracle client software on the Content Server computer.

PostgreSQL
To create a PostgreSQL database, see "Adding and Connecting to a New PostgreSQL Database" on page 281.

Microsoft SQL Server
To create a SQL Server database, see "Adding and Connecting to a New SQL Server Database" on page 283.

15.2.1 Adding and Connecting to a New SAP HANA Database

To create a new Content Server SAP HANA database, you use the utility functions on the **HANA Maintenance** page.

Creating a new Content Server SAP HANA database requires the following steps:

- “Logging onto HANA” on page 277 as a user with system access privileges
- “Creating a HANA Database User for Content Server” on page 277
- “Creating a HANA Schema” on page 278
- “Creating the Tables in the HANA Database” on page 278

Important
You must install the HANA database client on your Content Server computer before you connect to the HANA server to create a new Content Server HANA database.

Logging onto HANA

To open the **HANA Maintenance** page, where you can create your Content Server database and database user, and perform other database maintenance, log onto SAP HANA as a user with system administration privileges.

To log onto HANA:

1. On the **HANA Server Administrator Log-in** page, enter the host name and port, or IP address and port, of an SAP HANA server in the **HANA Server (IP:Port)** box. For example, enter `HANAserver.domain.com:30115` or `192.168.10.20:30115`.
2. Enter the name of an SAP HANA user with administrator privileges (for example, `SYSTEM`) in the **System User** box.
3. Type the password of the system user in the **System Password** box.
4. Click **Log-in**. After you successfully log on, the **HANA Maintenance** page appears.

Creating a HANA Database User for Content Server

Perform the following steps on the **HANA Maintenance** page, in the **Create A New User** section.

To create a HANA database user for Content Server:

1. Type the name of the new HANA user in the **User Name** box.
2. Type a password for the new HANA user in the **Password** box.
3. Type the password again in the **Verify Password** box.

4. Click **Create User**.

Creating a HANA Schema

Perform the following steps on the **HANA Maintenance** page, in the **Create A HANA schema** section.

To create a HANA schema:

1. In the **User Name** box, select the name of the user that you created in “Creating a HANA Database User for Content Server” on page 277.

2. In the **Schema** box, enter the name of the new HANA schema.

3. Click **Create Schema**.

After the tablespace is created, it is listed in the **Schema** menu in the **Delete a HANA schema** section of the **HANA Maintenance** page.

Creating the Tables in the HANA Database

To complete the creation of a new Content Server database, connect to the new Content Server database as the Content Server database user and create the Content Server database tables. Do this on the **Create Content Server Tables** page.

To return to the **Create Content Server Tables** page, click **Return to previous page** at the top of the **HANA Maintenance** page.

To create Content Server tables in a HANA database:

1. In the **HANA Schema** box, select the name of a HANA schema.

2. In the **HANA User Name** box, select the name of the HANA user that is associated with the HANA schema that you selected in step 1.

3. Enter the password of the HANA user in the **Password** box.

4. Optional Enable **External Document Storage** if you want Content Server to store documents and other items outside the database, and enter the absolute path of the folder where you want Content Server to store items in the adjacent box.

   Note: The directory that you enter must exist and the Content Server user must have permission to write to it.

5. Click **Create Tables**.

You have now created a new Content Server HANA database. You must now perform some configuration tasks to make Content Server ready to use. For information on these tasks, see “Configuring Content Server After Changing Your Database” on page 294.

15.2.2 Adding and Connecting to a New Oracle Database

To create a new Content Server Oracle database, you use the utility functions on the **Oracle Server Maintenance** page.

Creating a new Content Server Oracle database requires the following steps:

- "Logging onto Oracle Server" on page 279 as a user with system access privileges
- "Creating an Oracle Tablespace" on page 280
- "Creating an Oracle Database User for Content Server" on page 280
- "Creating the Tables in the Oracle Database" on page 281

Tip: If the option to create an Oracle database does not appear on the **Select RDBMS Type** page, ensure that you have installed Oracle client software on the Content Server computer.

Logging onto Oracle Server

To open the **Oracle Server Maintenance** page, where you can create your Content Server database and database user, and perform other database maintenance, log onto Oracle Server as a user with system administration privileges.

To log onto Oracle Server:

1. On the **Oracle Server Administrator Log-in** page, enter the name of an Oracle user with administrator privileges (for example, `system`) in the **System User Name** box.
2. Type the password of the system user in the **Password** box.
3. Type the service name (database alias) of Oracle Server in the **Service Name** box.

   Tip: The service name is typically the same as the host name of the computer on which Oracle Server is installed. You can find the service name (database alias) in the `tnsnames.ora` file. You may need to consult your Oracle administrator to obtain this information.

4. Click **Log-in**. After you successfully log on, the **Create Content Server Tables** page appears.

Creating an Oracle Tablespace

After you successfully log onto Oracle, the **Create Content Server Tables** page appears. Before you can create the Content Server tables, however, you must create a Content Server database and Content Server database user. You perform these tasks on the **Oracle Server Maintenance** page.

To open the **Oracle Server Maintenance** page, click the **Oracle Server Maintenance** link that appears in the **Note** near the top of the **Create Content Server Tables** page.

To create an Oracle tablespace:

1. On the **Oracle Server Maintenance** page, click **Create New Tablespace**.

2. Specify the characteristics of the tablespace.

   a. In the **Tablespace Name** box, type a unique name for the tablespace.

      Tip: You can find out which tablespace names are already in use by looking at the **Default Tablespace** menu in the **Create New User** section of this page.

   b. In the **File Specification** box, type the absolute path of the tablespace data file that you want to create. For example, `C:\oracle\database\filename.ora` or `/usr/oracle/database/filename.dbf`.

      The directory that you specify must already exist, and the Windows, Solaris, or Linux user that runs Oracle Server must have permission to write to it.

   c. In the **Size** box, type a size in megabytes for the tablespace data file.

   d. Optional Enable `Automatically extend tablespace`, if you desire.

3. Click **Create Tablespace**.

After the tablespace is created, it is listed in the **Default Tablespace** menu in the **Create A New User** section of the **Oracle Server Maintenance** page.

Creating an Oracle Database User for Content Server

To create an Oracle database user for Content Server:

1. On the **Oracle Server Maintenance** page, click **Create A New User**.

2. Specify the characteristics of the Content Server Oracle database user.

   a. Type the name of the new Oracle user in the **User Name** box.

   b. Type a password for the new Oracle user in the **Password** box.

   c. Type the password again in the **Verify Password** box.

   d. In the **Default Tablespace** menu, select the Oracle tablespace that you created in “Creating an Oracle Tablespace” on page 280

3. Click **Create User**.

Creating the Tables in the Oracle Database

To complete the creation of a new Content Server database, connect to the new Content Server database as the Content Server database user and create the Content Server database tables. Do this on the **Create Content Server Tables** page.

To return to the **Create Content Server Tables** page, click **Return to previous page** at the top of the **Oracle Server Maintenance** page.

To create Content Server tables in an Oracle database:

1. In the **User Name** menu, select the Oracle user that you created in "Creating an Oracle Database User for Content Server" on page 280.
2. Enter the password of the Oracle user in the **Password** box.
3. Optional Enable **External Document Storage** if you want Content Server to store documents and other items outside the database, and enter the absolute path of the folder where you want Content Server to store items in the adjacent box.

   Note: The directory that you enter must exist and the Content Server user must have permission to write to it.

4. Click **Create Tables**.

You have now created a new Content Server Oracle database, but you must perform some configuration tasks to make Content Server ready to use. For information on these tasks, see "Configuring Content Server After Changing Your Database" on page 294.

15.2.3 Adding and Connecting to a New PostgreSQL Database

To create a new Content Server PostgreSQL database, you use the utility functions on the **PostgreSQL Maintenance** page.

Creating a new Content Server PostgreSQL database requires the following steps:

- "Logging onto PostgreSQL" on page 282 as a user with system access privileges
- "Creating a PostgreSQL Database User for Content Server" on page 282
- "Creating a PostgreSQL Database" on page 282
- "Creating the Tables in the PostgreSQL Database" on page 283

Logging onto PostgreSQL

To open the **PostgreSQL Maintenance** page, where you can create your Content Server database and database user, and perform other database maintenance, log onto PostgreSQL as a user with system administration privileges.

To log onto PostgreSQL:

1. On the **PostgreSQL Server Administrator Log-in** page, enter the host name or IP address of a PostgreSQL server in the **PostgreSQL Server Name** box. For example, enter `PostgreSQLserver.domain.com` or `192.168.10.20`.
2. Enter the name of an PostgreSQL user with administrator privileges in the **System User** box.
3. Type the password of the system user in the **System Password** box.
4. Click **Log-in**. After you successfully log on, the **PostgreSQL Maintenance** page appears.

Creating a PostgreSQL Database

Perform the following steps on the **PostgreSQL Maintenance** page, in the **Create A New PostgreSQL Database** section.

To create a PostgreSQL database:

1. In the **Database Name** box, enter a name for your Content Server database.
2. Click **Create Database**.

After the database is created, it is listed in the **Delete a PostgreSQL Database** menu on the **PostgreSQL Maintenance** page.

Creating a PostgreSQL Database User for Content Server

Perform the following steps on the **PostgreSQL Maintenance** page, in the **Create A New User** section.

To create a PostgreSQL database user for Content Server:

1. Type the name of the new PostgreSQL user in the **User Name** box.
2. Type a password for the new PostgreSQL user in the **Password** box.
3. Type the password again in the **Verify Password** box.
4. Select the name of the database that you created in "Creating a PostgreSQL Database" on page 282.
5. Click **Create User**.

Creating the Tables in the PostgreSQL Database

To complete the creation of a new Content Server database, connect to the new Content Server database as the Content Server database user and create the Content Server database tables. Do this on the **Create Content Server Tables** page.

To return to the **Create Content Server Tables** page, click **Return to previous page** at the top of the **PostgreSQL Maintenance** page.

To create Content Server tables in a PostgreSQL database:

1. In the **PostgreSQL Database** box, select the name of a PostgreSQL database.
2. In the **PostgreSQL User Name** box, select the name of the PostgreSQL user that is associated with the PostgreSQL database that you selected in step 1.
3. Enter the password of the PostgreSQL user in the **Password** box.
4. Optional Enable **External Document Storage** if you want Content Server to store documents and other items outside the database, and enter the absolute path of the folder where you want Content Server to store items in the adjacent box.

   Note: The directory that you enter must exist and the Content Server user must have permission to write to it.

5. Click **Create Tables**.

You have now created a new Content Server PostgreSQL database. You must now perform some configuration tasks to make Content Server ready to use. For information on these tasks, see "Configuring Content Server After Changing Your Database" on page 294.

15.2.4 Adding and Connecting to a New SQL Server Database

To create a new Content Server SQL Server database, use the utility functions on the **Microsoft SQL Server Maintenance** page.

Important

Content Server cannot create a new database in a Microsoft Azure SQL database. To create the Content Server database, first create an empty database and a database user account on the Microsoft Azure Portal.

Note that, when you do not use Content Server to automatically create the Content Server database, you must configure the required and recommended settings manually. For example, you must enable the `READ_COMMITTED_SNAPSHOT` and `ALLOW_SNAPSHOT_ISOLATION` SQL Server isolation levels.

- For information on required and recommended settings for SQL Server databases, see Section 3.2.3 "Microsoft SQL Server Installation Guidelines" in *OpenText Content Server - Installation Guide (LLESCOR-IGD)*.

- For more information on connecting Content Server to an Azure SQL database that you have created for Content Server, see "Connecting to an Empty SQL Server Database" on page 290.

Creating a new Content Server SQL Server database requires the following steps:

- "Logging onto SQL Server" on page 284 as a user with system access privileges
- "Creating an Empty Microsoft SQL Server Database" on page 285
- "Creating a Content Server SQL Server Database User" on page 286
- "Creating the Tables in the SQL Server Database" on page 286

Logging onto SQL Server

To open the **Microsoft SQL Server Maintenance** page, where you can create your Content Server database and database user, and perform other database maintenance, log on to Microsoft SQL Server as a user with system administration privileges.

To log on to Microsoft SQL Server:

1. Type the Microsoft SQL Server alias in the **SQL Server Name** box.

   Tip: If your installation of Microsoft SQL Server does not run on the default port (1433), enter the SQL Server port after the server alias, separated by a comma, with no space.

   Example: For a SQL Server installation with an alias of `MySQLsrv` running on port 1456, enter the following in the **SQL Server Name** box:

   ```
   MySQLsrv,1456
   ```

2. Type the Microsoft SQL Server system administrator user name (the default is `sa`) in the **System User** box.
3. Type the password for the system user in the **System Password** box.
4. Type the name of the master database (the default is `master`) in the **Master Database Name** box.
5. Click **Log-in**. After you successfully log on, the **Create Content Server Tables** page appears.

Creating an Empty Microsoft SQL Server Database

After you successfully log on to Microsoft SQL Server, the **Create Content Server Tables** page appears. Before you can create the Content Server tables, however, you must create a Content Server database and Content Server database user. You perform these tasks on the **Microsoft SQL Server Maintenance** page.

To open the **Microsoft SQL Server Maintenance** page, click the **Microsoft SQL Server Maintenance** link that appears in the **Note** near the top of the **Create Content Server Tables** page.

To create a Microsoft SQL Server database:

1. On the **Microsoft SQL Server Maintenance** page, click **Create a New Microsoft SQL Server Database**.
2. Specify the characteristics of the database.
   a. In the **Database Name** box, type the name that you want to assign to the database, for example, `csdb`.

      Tip: You can find out which database names are already in use by looking at the **Database Name** menu in the **Create New User** section of this page.

   b. In the **Data File Specification** box, type a path and file name, for example, `C:\Store\csdb.mdf`.
   c. In the **Data File Size** box, type a size in megabytes for the Data File.
   d. Optional Enable `Automatically extend data file`, if you desire.
   e. In the **Log File Specification** box, type a path and file name, for example, `C:\Store\csdb.ldf`..
   f. In the **Log File Size** box, type a size in megabytes for the file.
   g. Optional Enable `Automatically extend log file`, if you desire.
3. Click **Create Database**.

After the database is created, it can be viewed in the **Database Name** menu in the **Create A New User** section of the **Microsoft SQL Server Maintenance** page.

Creating a Content Server SQL Server Database User

To create a Content Server SQL Server database user:

1. On the **Microsoft SQL Server Maintenance** page, click **Create A New User**.
2. Specify the characteristics of the Content Server SQL Server database user.
   a. Type the name of the new SQL Server user in the **User Name** box.
   b. Type a password for the new SQL Server user in the **Password** box.
   c. Type the password again in the **Verify Password** box.
   d. In the **Database Name** menu, select the SQL Server database that you created in "Creating an Empty Microsoft SQL Server Database" on page 285
3. Click **Create User**.

Creating the Tables in the SQL Server Database

To complete the creation of a new Content Server database, connect to the new Content Server database as the Content Server database user and create the Content Server database tables. Do this on the **Create Content Server Tables** page.

To return to the **Create Content Server Tables** page, click the **Return to previous page** link that appears at the top of the **Microsoft SQL Server Maintenance** page.

To create the tables in the Content Server SQL Server database:

1. In the **SQL Server Database** menu, select the Microsoft SQL Server database that you created in "Creating an Empty Microsoft SQL Server Database" on page 285.
2. In the **Microsoft SQL User Name** menu, select the Microsoft SQL Server user that you created in "Creating a Content Server SQL Server Database User" on page 286.
3. Enter the password of the Microsoft SQL Server user in the **Password** box.
4. Optional Enable **External Document Storage** if you want Content Server to store documents and other items outside the database, and enter the absolute path of the folder where you want Content Server to store items in the adjacent box.

   Note: The directory that you enter must exist and the Content Server user must have permission to write to it.

5. Click **Create Tables**.

You have now created a new Content Server SQL Server database. You must perform some configuration tasks to make Content Server ready to use. For information on these tasks, see "Configuring Content Server After Changing Your Database" on page 294.

15.3 Connecting to an Existing Database

To connect to an existing database, you require a Content Server database and a Content Server database user.

You can create an empty database and database user in advance, by using the <*RDBMS*> **Maintenance** page. The procedure is the same as described in “Adding and Connecting to a new Content Server Database” on page 276, except that you open the <*RDBMS*> **Maintenance** page directly from the **Content Server Administration** page. OpenText recommends that you proceed this way if you can because the Content Server database creation utility ensures that the database is created with required settings. For example, Content Server ensures that a SQL Server database is created with the required snapshot isolation levels.

You can also create an empty database and database user in advance by using only the tools of your RDBMS. (If you are creating a Content Server SQL Server database on Microsoft® Azure®, you are required to do so.) If you do not use Content Server to create your database, bear in mind that you are responsible for ensuring that your Content Server database has the required settings. For more information, see *OpenText Content Server - Installation Guide (LLESCOR-IGD)*.

If you connect to an empty database, you create the Content Server tables as part of the procedure of switching to an existing database. See “To Connect to an Existing Empty Database” on page 287

You can also connect to an existing database that already has Content Server tables. This is an important step in upgrading Content Server to a new version, but you might do it for other reasons too. For example, you might need to switch Content Server databases in a test environment. For instructions on switching from one Content Server to another, see “To Connect to an Existing Content Server Database” on page 291.

15.3.1 To Connect to an Existing Empty Database

During the process of changing your database, after you deselect your current database (see “Deselecting Your Current Database” on page 274), the **Database Administration** page appears, and you can connect to an existing empty database and create the Content Server tables in it.

To connect to an existing empty Content Server database, click **Create Tables in Existing Database**. On the **Select RDBMS Type** page, enable the type of database that you wish to connect to, and then click **Continue**.

SAP HANA
To connect to an SAP HANA database, see “Connecting to an Empty SAP HANA Database” on page 288.

Oracle
To connect to an Oracle database, see “Connecting to an Empty Oracle Database” on page 289.

PostgreSQL

To connect to a PostgreSQL database, see "Connecting to an Empty PostgreSQL Database" on page 289.

Microsoft SQL Server

To connect to a SQL Server database, see "Connecting to an Empty SQL Server Database" on page 290.

Connecting to an Empty SAP HANA Database

To connect to an empty SAP HANA database:

1. On the **Specify Content Server Database Owner** page, enter the host name and port, or IP address and port, of an SAP HANA server in the **HANA Server (IP:Port)** box. For example, enter `HANAserver.domain.com:30115` or `192.168.10.20:30115`.
2. Enter the name of the HANA user that owns the database that you wish to connect to in the **HANA User Name** box.
3. Enter the password of the HANA user in the **Password** box.
4. Enter the name of the HANA schema of the database that you wish to connect to in the **HANA Schema** box.
5. Click **Connect**. After you connect to the HANA server, the page refreshes and additional options appear, allowing you to create the tables for the Content Server database.
6. Optional Enable **External Document Storage** if you want Content Server to store documents and other items outside the database, and enter the absolute path of the folder where you want Content Server to store items in the adjacent box.

   Note: The directory that you enter must exist and the Content Server user must have permission to write to it.
7. Click **Create Tables**.

You have now connected to an existing Content Server HANA database and created the Content Server tables in it. You must now perform some configuration tasks to make Content Server ready to use. For information on these tasks, see "Configuring Content Server After Changing Your Database" on page 294.

Connecting to an Empty Oracle Database

To connect to an empty Oracle database:

1. On the **Specify Content Server Database Owner** page, enter the name of the Oracle user that owns the database that you wish to connect to.
2. Type the password of the user in the **Password** box.
3. Type the service name (database alias) of Oracle Server in the **Service Name** box.

   Tip: The service name is typically the same as the host name of the computer on which Oracle Server is installed. You can find the service name (database alias) in the `tnsnames.ora` file. You may need to consult your Oracle administrator to obtain this information.
4. Click **Connect**.
5. Optional The **External Document Storage** box appears. Enable **External Document Storage** if you want Content Server to store documents and other items outside the database, and enter the absolute path of the folder where you want Content Server to store items in the adjacent box.

   Note: The directory that you enter must exist and the Content Server user must have permission to write to it.
6. Click **Create Tables**.

You have now connected to an existing Content Server Oracle database and created the Content Server tables in it. You must now perform some configuration tasks to make Content Server ready to use. For information on these tasks, see "Configuring Content Server After Changing Your Database" on page 294.

Connecting to an Empty PostgreSQL Database

To connect to an empty PostgreSQL database:

1. On the **PostgreSQL Server Administrator Log-in** page, enter the host name or IP address of a PostgreSQL server in the **PostgreSQL Server Name** box. For example, enter `PostgreSQLserver.domain.com` or `192.168.10.20`.
2. Enter the name of the PostgreSQL user that owns the database that you wish to connect to in the **PostgreSQL User Name** box.
3. Enter the password of the PostgreSQL user in the **Password** box.
4. Enter the name of the PostgreSQL database that you wish to connect to in the **PostgreSQL Database** box.
5. Click **Connect**. After you connect to the PostgreSQL server, the page refreshes and additional options appear, allowing you to create the tables for the Content Server database.

6. Optional Enable **External Document Storage** if you want Content Server to store documents and other items outside the database, and enter the absolute path of the folder where you want Content Server to store items in the adjacent box.

   Note: The directory that you enter must exist and the Content Server user must have permission to write to it.

7. Click **Create Tables**.

You have now connected to an existing Content Server PostgreSQL database and created the Content Server tables in it. You must now perform some configuration tasks to make Content Server ready to use. For information on these tasks, see "Configuring Content Server After Changing Your Database" on page 294.

Connecting to an Empty SQL Server Database

To connect to an empty SQL Server database:

1. On the **Specify Content Server Database Owner** page, type the Microsoft SQL Server alias in the **SQL Server Name** box.

   Tip: If your installation of Microsoft SQL Server does not run on the default port (1433), enter the SQL Server port after the server alias, separated by a comma, with no space.

   Example: For a SQL Server installation with an alias of `MySQLsrv` running on port 1456, enter the following in the **SQL Server Name** box:

   ```
   MySQLsrv,1456
   ```

   For a SQL Server database server deployed on Azure, type the fully qualified domain name of the SQL Server database server. For example, enter `csdb.database.windows.net`.

   Tip: The SQL Server name, Microsoft SQL Server user name, and SQL database name of a SQL Server database deployed on Azure can be found in the **Connection strings** that appear in the **Essentials** of the SQL Server database server on your Azure dashboard.

2. In the **Microsoft SQL Server User Name** box, enter the name of the SQL Server user that owns the database that you wish to connect to.

   For a SQL Server database server deployed on Azure, enter the name of a user with administrative privileges. OpenText recommends that you use the name of the `Server admin login` that was created when the virtual SQL Server database server was created.

3. Type the password of the user in the **Password** box.

4. In the **SQL Server Database** box, type the name of the SQL Server database that you want to connect to.

5. Click **Connect**.

6. Optional The **External Document Storage** box appears. Enable **External Document Storage** if you want Content Server to store documents and other items outside the database, and enter the absolute path of the folder where you want Content Server to store items in the adjacent box.

   Note: The directory that you enter must exist and the Content Server user must have permission to write to it.

7. Click **Create Tables**.

You have now connected to an existing Content Server SQL Server database and created the Content Server tables in it. You must now perform some configuration tasks to make Content Server ready to use. For information on these tasks, see "Configuring Content Server After Changing Your Database" on page 294.

15.3.2 To Connect to an Existing Content Server Database

During the process of changing your database, after you deselect your current database (see "Deselecting Your Current Database" on page 274), the **Database Administration** page appears, and you can connect to an existing Content Server database that has Content Server tables in it.

To connect to an existing Content Server database, click **Select Existing Database**. On the **Select RDBMS Type** page, enable the database platform that you wish to connect to, and then click **Continue**.

Important

The database that you connect to should be from a Content Server environment that has the same modules installed as your current Content Server environment. If it is not, you will have to add or remove Content Server modules to match the database before you can use it in your current environment.

SAP HANA

To connect to an SAP HANA database, see "Connecting to a Content Server HANA Database" on page 292.

Oracle Server

To connect to an Oracle database, see "Connecting to a Content Server Oracle Database" on page 292.

PostgreSQL

To connect to a PostgreSQL database, see "Connecting to a Content Server PostgreSQL Database" on page 293.

Microsoft SQL Server

To connect to a SQL Server database, see "Connecting to a Content Server SQL Server Database" on page 293.

Connecting to a Content Server HANA Database

To connect to a Content Server HANA database:

1. On the **Specify Content Server Database Owner** page, enter the host name or IP address of a SAP HANA server in the **HANA Server Name** box. For example, enter `HANAserver.domain.com:30115` or `192.168.10.20:30115`.

2. Enter the name of the HANA user that owns the database that you wish to connect to in the **SAP HANA User Name** box.

3. Enter the password of the HANA user in the **Password** box.

4. Enter the name of the HANA database that you wish to connect to in the **HANA Database** box.

5. Click **Continue**.

6. On the **Content Server Administrator User Log-in** page, enter the password of the Content Server Admin user, and then click **Log-in**.

You have now connected to an existing Content Server HANA database. You must now perform some configuration tasks to make Content Server ready to use. For information on these tasks, see "Configuring Content Server After Changing Your Database" on page 294.

Connecting to a Content Server Oracle Database

To connect to a Content Server Oracle database:

1. On the **Specify Content Server Database Owner** page, enter the name of the Oracle user that owns the database that you wish to connect to.

2. Type the password of the user in the **Password** box.

3. Type the service name (database alias) of Oracle Server in the **Service Name** box.

   Tip: The service name is typically the same as the host name of the computer on which Oracle Server is installed. You can find the service name (database alias) in the `tnsnames.ora` file. You may need to consult your Oracle administrator to obtain this information.

4. Click **Continue**.

5. On the **Content Server Administrator User Log-in** page, enter the password of the Content Server Admin user, and then click **Log-in**.

You have now connected to an existing Content Server Oracle database. You must now perform some configuration tasks to make Content Server ready to use. For information on these tasks, see "Configuring Content Server After Changing Your Database" on page 294.

Connecting to a Content Server PostgreSQL Database

To connect to a Content Server PostgreSQL database:

1. On the **Specify Content Server Database Owner** page, enter the host name or IP address of a PostgreSQL server in the **PostgreSQL Server Name** box. For example, enter `PostgreSQLserver.domain.com` or `192.168.10.20`.

2. Enter the name of the PostgreSQL user that owns the database that you wish to connect to in the **PostgreSQL User Name** box.

3. Enter the password of the PostgreSQL user in the **Password** box.

4. Enter the name of the PostgreSQL database that you wish to connect to in the **PostgreSQL Database** box.

5. Click **Connect**.

6. On the **Content Server Administrator User Log-in** page, enter the password of the Content Server Admin user, and then click **Log-in**.

You have now connected to an existing Content Server PostgreSQL database. You must now perform some configuration tasks to make Content Server ready to use. For information on these tasks, see "Configuring Content Server After Changing Your Database" on page 294.

Connecting to a Content Server SQL Server Database

To connect to a Content Server SQL Server database:

1. On the **Specify Content Server Database Owner** page, type the Microsoft SQL Server alias in the **SQL Server Name** box.

   Tip: If your installation of Microsoft SQL Server does not run on the default port (1433), enter the SQL Server port after the server alias, separated by a comma, with no space.

   Example: For a SQL Server installation with an alias of `MySQLsrv` running on port 1456, enter the following in the **SQL Server Name** box:

   ```
   MySQLsrv,1456
   ```

   For a SQL Server database server deployed on Azure, type the fully qualified domain name of the SQL Server database server. For example, enter `csdb.database.windows.net`.

   Tip: The SQL Server name, Microsoft SQL Server user name, and SQL database name of a SQL Server database deployed on Azure can be found in the **Connection strings** that appear in the **Essentials** of the SQL Server database server on your Azure dashboard.

2. In the **Microsoft SQL Server User Name** box, enter the name of the SQL Server user that owns the database that you wish to connect to.

3. Type the password of the user in the **Password** box.
4. In the **SQL Server Database** box, type the name of the Microsoft SQL Server database that you want to connect to.
5. Click **Continue**.
6. On the **Content Server Administrator User Log-in** page, enter the password of the Content Server Admin user, and then click **Log-in**.

You have now connected to an existing Content Server SQL Server database. You must now perform some configuration tasks to make Content Server ready to use. For information on these tasks, see “Configuring Content Server After Changing Your Database” on page 294.

15.4 Configuring Content Server After Changing Your Database

After you change your Content Server database, Content Server displays a series of pages that direct you to perform configuration changes to ensure that Content Server is ready to use. Depending on the database operation that you have performed, you will see one, some or all of the following pages.

Database Upgrade

The **Content Server Database Upgrade Confirmation** page appears if the database that you connected to in “To Connect to an Existing Content Server Database” on page 291 needs to be upgraded. For information on upgrading the database, see “Upgrading the Content Server Database” on page 306 and *OpenText Content Server - Upgrade Guide (LLESCOR-IUP)*.

Configure OTDS Integration Settings

Content Server uses OpenText Directory Services for user management and authentication. The **Configure OTDS Integration Settings** page allows you to connect to an external OTDS server or use an OTDS server that is internal to Content Server.

User and Group Migration

On the **User and Group Migration** page, you can migrate existing internal Content Server users and groups to OTDS, or import users and groups using a `LDIF` file.

Typically, you migrate users and groups as part of your initial configuration of Content Server 16 or later after you upgrade a database from a deployment of Content Server 10.5 or earlier that manages users and groups within Content Server.

Note: The migration function on this page does not migrate users and groups from Content Server Directory Services. The migration function doesn't migrate CSDS users and groups. It migrates the CSDS sync profile into OTDS, which can then be used to import the same set of users.

For information on migrating users and groups from Content Server Directory Services, see *OpenText Directory Services - Installation and Administration Guide (OTDS-IWC)*.

Alternatively, if you selected Internal OTDS on the **Configure OTDS Integration Settings** page, you can import the users and groups that were previously exported from the same Content Server database that you just connected.

For more information on migrating or importing users and groups, see *OpenText Content Server - Administering OpenText Directory Services Integration Administration (LLESDSI-AGD)*.

Install Modules

The **Install Modules** page appears after you have successfully switched your Content Server database. It offers you the chance to install any available modules. For information on installing modules, see "Installing Modules" on page 413 and *OpenText Content Server - Module Installation and Upgrade Guide (LLESCOR-IMO)*

Admin Server Configuration

If you have connected to an existing Content Server database, after you click **Continue** on the **Install Modules** page, you are prompted to connect to a Content Server Admin server. After you log on to an Admin server, the **Configure and Migrate the Search System** page appears, which allows you to migrate an existing search index as part of a Content Server upgrade. For information on this page, see *OpenText Content Server - Upgrade Guide (LLESCOR-IUP)*.

If you have created a new Content Server database, after you click **Continue** on the **Install Modules** page, you are prompted to create a new Enterprise Data Source. For information, see *OpenText Content Server - Administering Search (LLESWBS-AGD)*.

License Setup

After you complete the Admin server configuration, you are presented with the **License Setup** page. For information on licensing Content Server and Content Server modules, see *OpenText Content Server - Installation Guide (LLESCOR-IGD)*.

Congratulations!

After you finish licensing Content Server (and Content Server modules, if applicable), the**Congratulations!** page appears, indicating that you have successfully changed your Content Server database and completed basic configuration of Content Server for the new database.

Chapter 16

Maintaining an Existing Database

The **Maintain Current Database** page displays information about the current Content Server database and provides links to a number of database-related administration pages.

16.1 Viewing Content Server Tables

A Content Server database stores data in a set of RDBMS tables. To view a list of these tables and the number of rows in them, click **View Content Server Tables** on the **Maintain Current Database** page. Additional information may be available depending on your database platform.

The **View Content Server Tables** page displays the following information:

Table 16-1: Information available on the View Content Server Tables page

	SAP HANA	Oracle	SQL Server	PostgreSQL
Table Name	✓	✓	✓	✓
Number of rows	✓	✓	✓	✓
Tablespace		✓		
Object Type		✓	✓	
Table or Object Owner		✓	✓	

16.2 Viewing Tablespace Usage (Oracle)

Oracle Database uses an entity called a *tablespace* to store the tables of one or more relational databases. A tablespace can have multiple database users, each owning a set of tables. In general, the set of tables corresponding to a Content Server database resides within a single tablespace, which it may share with other sets of tables owned by different database users.

If you use Oracle Database as your RDBMS, you can view the amount of space that is being used by Content Server tables in the Oracle tablespace.

To view Content Server tablespace usage, on the **Maintain Current Database** page, click **View Tablespace Usage**.

16.3 Performing Database Maintenance Tasks

To perform Content Server database maintenance tasks that are specific to your database platform, click <*RDBMS*> **Maintenance Tasks**. This opens the database maintenance for your database platform, where you can perform tasks that are related to the creation and maintenance of Content Server databases, such as creating a Content Server database and user, or deleting the tables within an existing Content Server database. The specific tasks that you can perform on the database maintenance page depend on your database platform.

After you click <*RDBMS*> **Maintenance Tasks**, you are prompted to log onto your database server as a user with database administrator privileges.

16.3.1 Performing HANA Maintenance Tasks

You can perform the following tasks on the **HANA Server Maintenance** page:

- Create a new HANA user
- Create a new HANA schema
- Delete a HANA schema

Typically, you create a HANA database and user as part of the procedure of creating a new Content Server database either during the initial setup of Content Server or afterwards.

For more information, see “Changing Your Content Server Database“ on page 273.

16.3.2 Performing Oracle Maintenance Tasks

You use the **Oracle Server Maintenance** page to perform the following tasks:

- Create a New Tablespace
- Create an Oracle User Account
- Extend a Tablespace
- Delete an Oracle User Account and/or its Tables

You use the **Oracle Server Maintenance** page under the following two circumstances:

- When you are administering an existing Content Server database. In this case you access the **Oracle Server Maintenance** page by clicking the **Oracle Server Maintenance Tasks** link on the **Maintain Current Database** page.
- When you are creating a new Content Server database to connect to a new or existing Content Server installation. In this case, you access the **Oracle Server Maintenance** page by clicking the **Oracle Server Maintenance** link on the **Create Content Server Tables** page.

Under either of the preceding circumstances, you click the **Return to previous page** link on the **Oracle Server Maintenance** page to return to the page (**Maintain Current Database** or **Create Content Server Tables**) from which you accessed the **Oracle Server Maintenance** page.

If you access the **Oracle Server Maintenance** page as part of the process of creating a new Content Server database, perform the following two tasks in the order shown before clicking the **Return to previous page** link:

- "Creating a New Tablespace" on page 299.
- "Creating a New Oracle User" on page 299.

Creating a New Tablespace

Content Server uses an Oracle *tablespace* to contain the tables of the Content Server database. Since a tablespace can contain tables owned by multiple Oracle users, it is not necessary to create a new tablespace if one with sufficient available space already exists.

Since a tablespace is created as part of the Content Server database creation procedure, it is normally not necessary to create one apart from that procedure.

Creating a New Oracle User

All of the tables in a tablespace are owned by Oracle users. A particular Oracle user owns the tables of the Content Server database. Content Server uses this Oracle user name and the corresponding password to connect to the Content Server database, which the Oracle Server manages.

An Oracle user is created as part of the Content Server database creation procedure, so it is normally not necessary to create a user apart from that procedure.

Extending a Tablespace

A tablespace consists of one or more datafiles. As the amount of data in your Content Server database grows, these datafiles may become full. You can increase the size of a tablespace by adding a new datafile to it.

Some versions of Oracle Database can be configured to extend tablespaces automatically when they run low on free space. For more information, consult the documentation that accompanied your Oracle Database software.

Deleting an Oracle User and the Tables It Owns

If a Content Server database becomes corrupt, the only way to recover it may be to delete its tables (and perhaps even the database user) and then restore the database from backup.

If you delete the tables only, tables created for custom categories are not removed. Therefore, you may want to delete both the user and its tables, which will remove the custom tables.

The **Oracle Server Administrator** Log-in page appears under the following two circumstances:

- You are creating a new Content Server database. The page appears after you click the **Continue** button on the **Select RDBMS Type** page.
- You clicked the **Oracle Server Maintenance Task** link on the **Maintain Current Database** page.

The purpose of this page is to prompt you to specify the user name and password of an RDBMS account that has administrator privileges.

To Create a New Tablespace

To create a new tablespace:

1. On the **Oracle Server Maintenance** page, click the **Create New Tablespace** link.
2. Type a unique name for the tablespace (for example, `_TS`) in the **Tablespace Name** field.

   You can find out what tablespace names are already in use in the **Default Tablespace** drop-down list in the **Create New User** section of the **Oracle Server Maintenance** page.
3. In the **File Specification** field, type the absolute path of the tablespace datafile that you want to create (for example, `C:\orant\database\filename.ora` or `/usr/oracle/database/filename.dbf`). The directory that you specify must already exist and the operating system user created for Oracle Database must have permission to write to it.
4. In the **Size** field, type a size in MB for the tablespace datafile (the minimum is 5MB), following the guidelines in the **Create New Tablespace** section on the **Oracle Server Maintenance** page.
5. Click the **Create Tablespace** button.
6. Do one of the following:

   - If you are creating a new Content Server database and have not yet created the Oracle user, go to "To Create an Oracle User" on page 301.
   - If you have completed all tasks on the **Oracle Server Maintenance** page, click the **Return to previous page** link.

To Create an Oracle User

To create an Oracle user:

1. On the **Oracle Server Maintenance** page, click **Create New User**.
2. In the **Create New User** section, type a unique name for the Oracle user in the **User Name** field.
3. In the **Password** field, type a password for this user and type it again in the **Verify Password** field
4. In the **Default Tablespace** list, click the name of the tablespace in which you want to create the tables of the new Content Server database.
5. Click the **Create User** button.
6. Do one of the following:
   - If you are creating a new Content Server database, click the **Return to previous page** link to return to the Create Content Server Tables page.
   - Otherwise, if you have completed all tasks on the **Oracle Server Maintenance** page, click **Return to previous page** to return to the **Maintain Current Database** page.

To Extend an Oracle Tablespace

To extend an existing tablespace:

1. On the **Oracle Server Maintenance** page, click **Extend Tablespace**.
2. In the **Tablespace To Extend** list, click the name of the tablespace that you want to extend.
3. In the **File Specification** field, type the absolute path of the file that you want to use for the tablespace datafile extension (for example, `C:\orant\database\filename.ora` or **`Oracle Server Maintenance`**`/usr/oracle/database/filename.dbf`). The directory that you specify must already exist and the operating system user created for Oracle Database must have permission to write to it.
4. In the **Size** field, type a size in MB for the new tablespace datafile. Based on the size of previous datafiles that have been created for this tablespace and the time that it took to fill them, you can estimate an appropriate size for the new tablespace datafile.
5. Click the **Extend Tablespace** button.
6. If you have completed all tasks on the **Oracle Server Maintenance** page, click **Return to previous page**.

To Delete Oracle Users and Tables

To delete an Oracle user or tables:

1. On the **Oracle Server Maintenance** page, click **Delete Users and Tables**.
2. In the **User Name** list, click the name of the Oracle user that you want to delete or whose tables you want to delete.
3. Do one of the following:
   - To delete the selected Oracle user *and all the tables that it owns*, click the **Delete user and tables** radio button.
   - If you want to delete *only the Content Server tables* owned by the selected Oracle user, click the **Delete tables only** radio button.
4. Click the **Delete** button.
5. Click the **OK** button in the dialog box that opens.
6. If you have completed all tasks on the **Oracle Server Maintenance** page, click **Return to previous page**.

16.3.3 Performing SQL Server Maintenance Tasks

The **Microsoft SQL Server Administrator Log-in** page appears under the following circumstances:

- You are creating a new Content Server database. The page appears after you click the **Continue** button on the **Select RDBMS Type** page.
- You clicked the **Microsoft SQL Server Maintenance Tasks** link on the **Maintain Current Database** page.

The purpose of this page is to prompt you to specify the user name and password of an RDBMS account that has administrator privileges.

Use the **Microsoft SQL Server Maintenance** page to perform the following tasks:

- Create a new Microsoft SQL Server database
- Create a new user
- Extend a Microsoft SQL Server database
- Delete Microsoft SQL Server Content Server tables
- Delete a Microsoft SQL Server database

Use the **Microsoft SQL Server Maintenance** page under the following two circumstances:

- When you are administering an existing Content Server database. In this case, you access the **Microsoft SQL Server Maintenance** page by clicking the

Microsoft SQL Server Maintenance Tasks link on the **Maintain Current Database** page.

Under either of the preceding circumstances, you click the **Return to previous page** link on the **Microsoft SQL Server Maintenance** page to return to the page (**Maintain Current Database** or **Create Content Server Tables**) from which you accessed the **Microsoft SQL Server Maintenance** page.

Deleting Content Server Tables or a SQL Server Database

If your Content Server database becomes corrupt for some reason, the only way to recover it may be to delete its tables or even the SQL Server database in which they reside and then restore them from backup.

Extending a SQL Server Database

As the amount of data in a SQL Server database approaches the maximum space allotted to the database in data file, you will need to increase the amount of space allotted in the data file to extend the database. You can allot space in more than one data file to a SQL Server database.

To Extend a SQL Server Database

To extend a SQL Server database:

1. On the Administration page, select **Database Administration**.
2. On the Database Administration page, select **Maintain Current Database**.
3. On the Maintain Current Database page, select **Microsoft SQL Server Maintenance Tasks**. You may need to enter your SQL Server administrator password.
4. On the **Microsoft SQL Server Maintenance** page, click **Extend a Microsoft SQL Server Database**.
5. In the **Database to Extend** list, click the name of the SQL Server database that you want to extend.
6. In the **Data File** list, click the name of the data file in which you want to allot more space to this SQL Serverdatabase.
7. In the **Data File Allotment** field, type the amount of additional data file space (in MB) that you want to allot to this SQL Server database.
8. Click the **Extend Database** button.
9. If you have completed all desired tasks on the **Microsoft SQL Server Maintenance** page, click **Return to previous page**.

To Delete Content Server Tables

To delete Content Server tables:

1. On the Administration page, select **Database Administration**.
2. On the Database Administration page, select **Maintain Current Database**.
3. On the Maintain Current Database page, select **Microsoft SQL Server Maintenance Tasks**. You may need to enter your SQL Server administrator password.
4. On the **Microsoft SQL Server Maintenance Tasks** page, click **Delete Microsoft SQL Server Content Server Tables** link.
5. In the **Database Name** drop-down list, click the name of the SQL Server database that contains the Content Server tables that you want to delete.
6. In the **User Name** drop-down list, click the name of the SQL Server user that the Server uses to log into this SQL Server database.
7. Type the password of the SQL Server user in the **Password** field.
8. Click the **Delete Tables** button.
9. Click the **OK** button in the dialog box that opens.
10. If you have completed all desired tasks on the **Microsoft SQL Server Maintenance Tasks** page, click the **Return to previous page** link.

To Delete a SQL Server Database

To delete a SQL Server database:

1. On the **Microsoft SQL Server Maintenance Tasks** page, click **Delete a Microsoft SQL Server Database**.
2. In the **Database Name** drop-down list, click the name of the SQL Server database that you want to delete.
3. Click the **Delete Database** button.
4. Click the **OK** button in the dialog box that opens.
5. If you have completed all desired tasks on the **Microsoft SQL Server Maintenance Tasks** page, click **Return to previous page**.

16.3.4 Performing PostgreSQL Maintenance Tasks

You can perform the following tasks on the **PostgreSQL Maintenance** page:

- Create a PostgreSQL database for use with Content Server
- Create a PostgreSQL user for use with Content Server
- Delete the Content Server tables from a PostgreSQL database
- Delete a PostgreSQL database

Typically, you create a PostgreSQL database and user as part of the procedure of creating a new Content Server database either during the initial setup of Content Server or afterwards.

For more information, see "Changing Your Content Server Database“ on page 273.

16.4 Purging Deleted Data (Oracle)

The **Maintain Current Database** page displays the **Purge Delete Data** link if you are using Oracle Database as your RDBMS and the Content Server database uses internal document storage.

When users delete documents form the Content Server database, Oracle marks the data as *deleted*, but it is still taking up disk space. OpenText recommends that you purge this deleted data periodically to recover disk space.

The **Purge Deleted Data** link opens the **Purge Deleted Data** page, on which you perform the purge operation.

If you are using Oracle Database as your RDBMS and your Content Server database stores documents internally, you can use the **Purge Deleted Data** page to remove data marked as *deleted* from the BLOB data table. You access the **Purge Deleted Data** page by clicking **Purge Deleted Data** on the **Maintain Current Database** page.

When a Content Server user deletes a document stored internally in a Content Server database, Oracle does not delete the document from the storage media, but rather marks the document as *deleted*. Thus, the document continues to use up disk space, even though Content Server users can no longer access it. For this reason, OpenText recommends that you purge your Content Server database of deleted data periodically to free disk space.

Purging deleted data requires that you have enough *rollback segments* to purge the BLOB data table. For more information about rollback segments, consult your Oracle documentation.

16.5 Upgrading the Database

The **Content Server Database Upgrade Confirmation** page provides information on your Content Server database schema and indicates whether any database upgrades are available. If your database is up to date, the **Content Server Database Upgrade Confirmation** page displays the current schema version of the Content Server database and of the modules that use tables in the Content Server database.

You access the **Content Server Database Upgrade Confirmation** page by clicking **Upgrade this Database** on the **Maintain Current Database** page. It may also appear automatically during an upgrade or module installation.

If the **Content Server Database Upgrade Confirmation** page indicates that there are database upgrades available, you should upgrade the Content Server database.

16.5.1 Upgrading the Content Server Database

To upgrade the Content Server Database:

1. On the **Content Server Database Upgrade Confirmation** page, enable **Upgrade the <*DB_name*> Content Server database**, and then click **Continue**.

2. On the **Admin Server Configuration** page, change the **Host Name**, **Port Number** and **Password** of the listed Admin servers, if necessary, so that these values are correct for the Admin servers in your environment, and then select the **Accept** check box.

   Note: If an Admin server **Status** is `Unavailable`, make sure that it is running before you proceed. You must select the **Accept** check box for every Admin server before you can start the upgrade process.

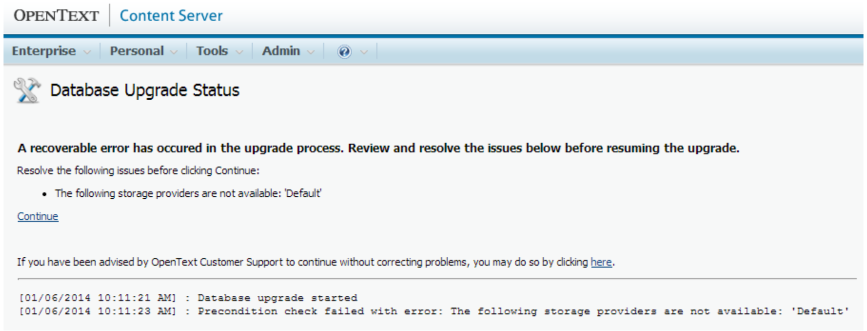
   Click **Continue** when you have made the necessary changes.

3. When the **Restart Content Server** page appears, click **Restart** to restart Content Server automatically (or click **Continue** if you prefer to restart Content Server using the operating system.)

4. When the **Restart Successful** message appears, click **Continue**. The **Database Upgrade Status** page appears. It displays the progress of the upgrade and refreshes its display every few seconds.

5. On the **Database Upgrade Status** page, a series of messages appear that indicate the progression of your database upgrade.

   Important
   If Content Server indicates that a recoverable error has occurred in the upgrade process, correct the issue and then click **Continue**.



Database Upgrade Status

A recoverable error has occured in the upgrade process. Review and resolve the issues below before resuming the upgrade.

Resolve the following issues before clicking Continue:

- The following storage providers are not available: 'Default'

Continue

If you have been advised by OpenText Customer Support to continue without correcting problems, you may do so by clicking here.

```
[01/06/2014 10:11:21 AM] : Database upgrade started
[01/06/2014 10:11:23 AM] : Precondition check failed with error: The following storage providers are not available: 'Default'
```

On the bottom of the **Database Upgrade Status** page, verify that the message `The database upgrade completed with no errors` appears. If the database upgrade completes successfully, and no errors are present, click **Continue**.

Important

Review the text on the page carefully. Occasionally the **Database Upgrade Status** page may display the message `"The database upgrade has completed successfully` when the page also displays messages indicating the occurrence of errors that were not sufficient to halt the database upgrade.

If any errors appear, do not attempt to continue the upgrade or restart the upgrade where it left off. Contact OpenText Customer Support.

16.6 Verifying the Database

If you are experiencing difficulty with your Content Server database, you can use the diagnostic tests on the **Verify Content Server Database** page to verify various aspects of the database. You access the **Verify Content Server Database** page by clicking the **Verify This Database** link on the **Maintain Current Database** page.

You can run both predefined and custom diagnostic test sets.

16.6.1 Managing Custom Verification Options

Running Predefined Diagnostic Test Sets

The **Verify Content Server Database** page displays five radio buttons (**Level 1 Diagnostic** to **Level 5 Diagnostic**) that you click to select the desired test set. The tests performed at each level are listed below each radio button.

Running a Custom Set of Diagnostic Tests

If none of the predefined diagnostic test sets meet your needs, you can go to the **Custom Verification Options** page to select a custom set of diagnostic tests to perform.

You can access the **Custom Verification Options** page by clicking the **Go To Custom Verification Options** link on the **Verify Content Server Database** page.

Depending on whether your database uses internal or external document storage, Content Server displays a different set of test options.

The **Initial Content Server Database Verification Report** page appears after you click the **Perform Diagnostic** button on either the **Verify Content Server Database** page or the **Custom Verification Options** page (internal or external storage version).

The **Initial Content Server Database Verification Report** page informs you that the verification is in progress and displays a link that you can click to view the status/ results of the verification.

The second **Content Server Database Verification Report** page appears after you click the **click here** link on the initial **Content Server Database Verification Report** page.

If the verification is in progress, the second **Content Server Database Verification Report** page displays the status of the verification. If the verification is complete, the page displays the results of the verification. If no errors are found, the page displays the message, "Congratulations! No errors were found in this database."

Custom Verification Options

You access the **Custom Verification Options** page by clicking the **Go To Custom Verifications Options** link on the **Verify Content Server Database** page.

The set of tests that appear depends on whether your Content Server database is set to store documents internally or externally. This help topic lists the tests available for an internal-storage database. The tests available for an external-storage database are also available.

If none of the predefined diagnostic test sets on the **Verify Content Server Database** page meet your needs, select a custom set of diagnostic tests to perform on the **Custom Verification Options** page.

To Run Custom Diagnostic Tests on the Database (Internal)

To run a custom set of diagnostic tests on your Content Server database:

On the Custom Verification Options page, select any of the following check boxes:

1. Verify the ACL count of a node
2. Verify the child count of a container
3. Verify that a DataID exists for each DocID
4. Verify that a ProviderData providerID exists for each providerID on DVersData
5. Verify the existence of members and leaders of groups
6. Verify that each group recorded on KUAFChildren exists
7. Search for nodes without ParentIDs

8. Verify the parentID of each node
9. Verify that a DVersData providerID exists for each providerID on ProviderData
10. Click the **Perform Diagnostic** button.

To Run Custom Diagnostic Tests on the Database (External)

To run a custom set of diagnostic tests on your Content Server database:

1. On the Custom Verification Options page, select any of the following check boxes:
   - Verify the ACL count of a node
   - Verify the child count of a container
   - Verify that a DataID exists for each DocID
   - Verify that a ProviderData providerID exists for each providerID on DVersData
   - Verify the file size of the external document store
   - Verify that each file represented on the ProviderData table exists in the external document store
   - Verify the name of each file in the external document store
   - Verify the existence of members and leaders of groups
   - Verify that each group recorded on KUAFChildren exists
   - Search for nodes without ParentIDs
   - Verify the parentID of each node
   - Verify that a DVersData providerID exists for each providerID on ProviderData
2. Click the **Perform Diagnostic** button. The Initial Content Server Database Verification Report page appears.

To Run Predefined Diagnostic Tests on the Database

To run predefined diagnostic tests on the database:

1. On the Verify Content Server Database page, click the radio button of the diagnostic test set that you want to perform.
2. Click the **Perform Diagnostic** button to display the initial Content Server Database Verification Report page.

16.6.2 Rebuilding Ancestor Tables

Important

OpenText recommends that you **do not** access these URLs unless specifically directed to by OpenText technical support.

The Content Server administration pages described in this section are used to rebuild the ancestor database tables in Content Server. Rebuilding the ancestor tables is accomplished by typing the following URLs in your browser:

1. **http://<***Content Server_IP_address***>/OTCS/cs.exe?func=admin.AskRebuildAncestors**

   The `admin.AskRebuildAncestors` URL will display the **Enable the Ancestor Agent** administration page. The **Enable the Ancestor Agent** page allows you to optionally trigger `http://`*`<Content Server_IP_address>`*`/OTCS/cs.exe?func=admin.RebuildAncestors`.

   Click **OK** to rebuild the tables.

   The **Enable the Ancestor Agent** page will update during the rebuild, and the URL will change to `http://`*`<Content Server_IP_address>`*`/OTCS/cs.exe?func=admin.RebuildAncestorLog`. Wait until you see the message “The rebuild of the Ancestor tables has completed successfully.”.
2. **http://<***Content Server_IP_address***>/OTCS/cs.exe?func=admin.RebuildAncestors**

   The `admin.RebuildAncestors` URL is used to rebuild the DTreeAncestors and / or the DBrowseAncestors table. It takes an optional, target parameter:

   - `DTA` will rebuild DTreeAncestors
   - `DBA` will rebuild DBrowseAncestors
   - If no target is specified, both tables will be rebuilt.

   The **Enable the Ancestor Agent** page will appear and will update during the rebuild. The URL will change to `http://`*`<Content Server_IP_address>`*`/OTCS/cs.exe?func=admin.RebuildAncestorLog`. Wait until you see the message “The rebuild of the Ancestor tables has completed successfully.”.
3. **http://<***Content Server_IP_address***>/OTCS/cs.exe?func=admin.RebuildAncestorLog**

   The `admin.RebuildAncestorLog` URL will monitor the status of the rebuilding of the ancestors table(s). The two URLs above will redirect to this URL after triggering a rebuild.

16.7 Testing or Repairing Known Database Issues

The **Test or Repair Known Database Issues** page contains Content Server database test and repair utilities. New utilities are added by Content Server Updates. Be careful with these correction utilities! Use them only if you are confident that they resolve specific error conditions that were detected by a Database Verification.

Repair items with blank multilingual names

This utility locates items that have blank names (empty strings) for each metadata language that you have deployed in Content Server. It updates the blank names with NULL values, which allows Content Server's language logic to function correctly. After you run **Repair items with blank multilingual names**, the missing name is displayed in another language (normally the system default language) until a valid name is entered to replace the NULL value.

Identify Duplicate ACL Permissions

This utility locates sets of database rows that contain an Access Control List (ACL) for the same Content Server item. It offers several methods of consolidating the rows into a single ACL entry. You can consolidate duplicate ACLs in a bulk operation or one at a time.

Remove duplicate ACLs in bulk

- **Eliminate exact duplicates**

  The safest option. It removes only ACLs that are exact copies of each other, and has no effect on user or group permissions. Duplicate ACLs that are not exact copies of each other are not affected by this operation.

  Example: There are two ACLs giving User1 the `See` permission for `CorpDoc01`. Running **Eliminate exact duplicates** removes one of them.

  Typically, after you run **Eliminate exact duplicates**, you address any remaining duplicate ACLs using one of the remaining methods.

- **Remove all duplicates**

  If a user or group has permissions for an item in multiple ACLs, every duplicate ACL is removed. Users and groups lose permissions as a result of this operation.

  Example: There are two ACLs giving User2 the following permissions for `CorpDoc02`:

  - **ACL1**

    `See`, `See Contents`

  - **ACL2**

    `See`, `See Contents`, `Modify`, `Reserve`

Running **Remove all duplicates** removes both ACLs. After it is run, User2 does not have permission to access `CorpDoc02`.

- **Use effective permissions**

  If a user or group has permissions for an item in multiple ACLs, the permissions are combined. No users or groups lose permissions as a result of this operation.

  Example: There are two ACLs giving User3 the following permissions for `CorpDoc03`:

  - **ACL1**

    `See`, `See Contents`, `Modify`, `Edit Attributes`, `Delete Versions`, `Delete`

  - **ACL2**

    `See`, `See Contents`, `Modify`, `Reserve`

  Running **Use effective permissions** combines both ACLs. After it is run, User3 has the following permissions for `CorpDoc03`: `See`, `See Contents`, `Modify`, `Edit Attributes`, `Reserve`, `Delete Versions`, `Delete`

Remove duplicate ACLs individually

To repair duplicate ACLs one at a time, click the **DataID** of the item that has multiple ACLs. The **Permissions** page for the item opens and the user or group that has multiple ACLs appears with *** Needs review *** beside it. To consolidate the ACLs for this user or group, select the user or group and enable the correct permissions under **Edit User Permissions**. Click **Repair** to consolidate the permissions into a single ACL entry.

Relocate Orphaned Items

Orphaned items are items that do not have a reference to a valid parent container in the database. For example, if the database does not contain a valid reference to a document’s parent folder, the document is an orphaned item. The **Relocate Orphaned Items** utility identifies orphaned items and gives you the option of moving them to a special volume, the **Orphaned Items Volume**.

Once items are in the **Orphaned Items Volume**, you can do whatever you want with them. You can move, copy, or delete them, or perform any other operation permitted by their item types.

Insert Missing Reflexive Rows for Volume Objects

This utility uses the results from a Level 5 Database verification to identify and insert missing reflexive rows into the `DTreeAncestors` table for volume objects.

Regenerate ChildCounts

This utility regenerates corrected `ChildCount` column values in the `DTreeCore` table.

Regenerate ACLCounts

This utility regenerates corrected `ACLCount` column values in the `DTreeCore` table.

Delete references to nonexistent Users and Groups

This utility uses the User & Group verification queries from the Database Verification functionality to present a possibly truncated list of references in the `KUAFChildren` table to delete users or groups that do not exist in the `KUAF` table, and provides you with the ability to delete these entries. For details, see "Managing Custom Verification Options" on page 307.

Directly deleting a user or group that do not exist in the KUAF table also causes a change to other referentially stored database information in a number of associated tables. Users or groups should not be deleted directly in Content Server because this can lead to unexpected consequences.

Delete orphaned rows in DVersData

This utility uses the `DocIDs` and `ProviderIDs` verification queries from the Database Verification functionality to present a list of orphaned rows in the `DVersData` table, and allows you to delete the `DocID` and `ProviderID` entries that do not exist.

Delete references to nonexistent Objects

This utility uses the Database Verification functionality to present a list entries in the `DTreeAncestors` table which reference nonexistent Objects, and allows you to delete these Objects.

Identify Document Class Cycles

Dependency cycles can be created, accidentally, in the **Document Class** definitions that are used to build Facets. These cycles can cause recursion problems when building Document Class facets, and can cause an error indicating that the maximum recursion limit has been exceeded.

The **Identify Document Class Cycles** option has been included on the **Test or Repair Known Database Issues** page to check for these dependency cycles.

To view or run installed database test and repair utilities:

1. On the Content Server Administration page, under **Database Administration**, click **Maintain Current Database**.
2. On the **Maintain Current Database** page, click **Test or Repair Known Database Issues**.
3. On the **Test or Repair Known Database Issues** page, click the utility you want to view or run.

To check for dependency cycles in document class definitions:

1. On the Content Server Administration page, under **Database Administration**, click **Maintain Current Database**.
2. On the **Maintain Current Database** page, click **Test or Repair Known Database Issues**.
3. On the **Test or Repair Known Database Issues** page, click **Identify Document Class Cycles**.
4. The **Content Server Database Verification Report** page appears. It will either confirm that the diagnostic test found no document class cycles, or it will inform you of the number of document class cycles found in your database.
5. If document class cycles have been found, select the links provided in the report to fix the records in the database:

   a. Identify which relationship should be removed for each loop. Each link will take you to the page where the relationship is defined. You will only need to remove one.

   b. Next to the relationship you need to remove, either clear the associated box, or click '-'.

   c. Click **Update**.
6. Re-run the **Identify Document Class Cycles** diagnostic tool.

16.8 Changing the Password of the Content Server Database User

During the setup of Content Server, you create a Content Server database and a Content Server database user. Typically, you perform both of these steps on the **Database Maintenance** page. (See “Changing Your Content Server Database“ on page 273.)

When you create a Content Server database user, you give it a name and password, and make it the owner of the Content Server database. Content Server stores the Content Server database user name and password and uses it to establish a database connection. If the password of the database user does not change, the stored credentials allow Content Server to connect to the Content Server database whenever necessary.

Over time, however, the password of the Content Server database user might be updated. The database user’s password might be changed, for example, by a database administrator who is following your organization’s security procedures, or through some other mechanism. However the change occurs, once the database user’s password is changed, the information stored in Content Server is no longer valid and Content Server cannot connect to its database. To allow Content Server to connect to the database, you must update the Content Server database user’s password on the **Update Database Connection Password** page.

Note: Changing the password on the **Update Database Connection Password** page changes the password that Content Server stores to enable its database user to connect. It does not change the password of the database user on the RDBMS.

16.8.1 To Change the Password Used to Connect to the Database

To change the password used to connect to the database:

1. In the **Database Administration** section of the Content Server Administration page, click **Maintain Current Database**.
2. On the **Maintain Current Database** page, click **Update Database Connection Password**.
3. On the **Update Database Connection Password** page, enter the current (changed) password of the Content Server database user.
4. Click **Update Password**.
5. On the **Restart Content Server** page, click **Restart** to restart Content Server automatically, or click **Continue** if you prefer to use the operating system to restart Content Server.

Chapter 17

Administering Blob Deletion Failures

The Flexible Storage Management module enables tracking of blob deletion errors. You can monitor blob deletion errors and attempt to delete the blobs that failed to delete on previous deletion attempts. If a deletion failure is detected, the Administer Blob Deletion Failures page lists information about the blob deletion, such as its Logical Provider name, the class of the error, and the error string associated with the deletion failure, if one exists. This page provides you with the date and time the next automated attempt to delete the blob will occur, and gives you the date that the failure was queued.

If you want to manually retry to delete blobs, you can do so on the Administer Blob Deletion Failures page. However, it is possible that manual blob deletion attempts can fail, just as automated attempts can fail.

Note: Blobs that are not deleted because the physical storage retention period is not yet expired are not available for manual deletion retries.

Administrators can view the scheduled activity for retrying blob deletion failures, and set the schedule to a specific day and time when they want to the Provider Blob Deletion Failure Retry Agent to run. When the retry agent runs, it processes log file entries, inserting those entries into the ProviderRetry database table. The log files contain blob deletion failure entries that the system attempted to insert into the ProviderRetry database table, but failed. The retry agent then searches for blob deletion records more than 24 hours old. The retry agent then attempts to delete each blob deletion failure entry listed in the ProviderRetry database table.

Note: By default, the Provider Blob Deletion Failure Retry Agent schedule is set to run every night at 12:00 a.m.

Blob deletion failures are events that can be audited by Content Server. The following events can be audited:

- **Provider Retry Deleted**, which is created when a blob that could not initially be deleted is successfully deleted.
- **Provider Retry Queued**, which is created when a blob deletion fails and a row in the ProviderRetry database table is either inserted or updated.
- **Provider Queuing Error**, which is created when a blob deletion fails and the system is unable to either insert a row into the ProviderRetry table or add a row to the log file indicating that the blob deletion failed.
- **Provider Retry Retried**, which is created whenever the system attempts to delete a blob that previously could not be deleted.

For more information about event auditing, see "Administering Event Auditing" on page 319.

17.1 To Monitor Blob Deletion Failures

To monitor Blob Deletion Failures:

1. In the **System Administration** section on the Administration page, click the **Administer Blob Deletion Failures** link.
2. On the Administer Blob Deletion Failures page, click the **Monitor Blob Deletion Failures** link.

   Optionally, select the check box for each blob you want to reattempt to delete, and then click the **Retry Now** button.

17.2 To Configure the Provider Blob Deletion Failure Retry Agent

To configure the Provider Blob Deletion Failure Retry Agent:

1. In the **System Administration** section on the Administration page, click the **Configure the Provider Blob Deletion Failure Retry Agent** link.
2. In the Provider Blob Deletion Failure Retry section on the Configure Scheduled Activities page, do the following:
   - Click the Enable radio button.
   - In the **Activity Schedule** section, select the days and times you want the Provider Blob Deletion Failure Retry agent to run.
3. Click the **Submit** button.

Chapter 18

Administering Event Auditing

Content Server allows you to track events that occur in the Content Server database.

Tip: An `event` is any action that users perform on a Content Server item, such as a document or folder.

Auditing events lets you monitor how Content Server users are using the system and determine who has performed certain operations. For example, you can identify which users have deleted or moved items.

In general terms, Content Server auditing involves:

Setting audit interests

You can choose the events that Content Server audits. To set audit interests, you must have the `System administration rights` privilege and the `Web Admin` usage privilege. For more information, see:

- "To Set Auditing Interests" on page 326
- "To View All Currently Set Auditing Interests" on page 327

Viewing and managing audit records

You can query the audit log and purge it of events. In specific cases, you may want to convert or purge older audit information that is stored in an obsolete format. To query the audit log, you must have the `Query Audit Log` usage privilege. (The `Query Audit Log` usage privilege is one of the "Business Administration Usage Privileges" on page 347.) To purge the audit log or to manage audit records created in prior releases, you must have the `System administration rights` privilege and the `Web Admin` usage privilege. For more information, see:

- "To Query the Audit Log" on page 328
- "To Purge the Audit Log" on page 329
- "To Manage Audit Records Created in Prior Releases" on page 330

Managing audit security settings

To prevent unauthorized employees from viewing the audit log and ensure its integrity, you may wish to enable additional audit security settings. To manage audit security settings, you must log on as the Content Server Admin user. For more information see:

- "To Configure Audit Security Settings" on page 332

18.1 Managing Audit Interests

On the **Set Auditing Interests** page, you can specify the events that Content Server audits. "Auditable Events" on page 320 lists the events that are available to audit when Content Server is installed. Optional modules often add new events that Content Server can audit.

Note: When an audit event is not registered with the registry subsystem, it is logged as *Deprecated*. A deprecated audit event has an ID of zero (0).

You can also enable settings that affect the functioning of the Audit system.

Force auditing of all events performed by System Administrators

When you enable this option, you ensure that any auditable actions performed by a System Administrator (users that have the System Administration privilege) are recorded, regardless of which events you have enabled on the **Set Auditing Interests** page.

Audit an "Attributes Changed" event for Category Attributes modified during item creation

This option affects how Content Server records `Attributes Changed` events. It has no effect if the `Attributes Changed` auditing interest is not enabled.

Enabled (default setting)

If the option is enabled, an `Attributes Changed` event is recorded when an item (or item version) that is created or copied has a Category Attribute applied to it, and the default value of the Category Attribute is changed.

It does not matter whether the Category Attribute is inherited from a parent container or explicitly applied by a user. An `Attributes Changed` event is recorded only if a user changes the Category Attribute from its default value. If the user does not change the default value of the Category Attribute, an `Attributes Changed` event is not recorded.

Disabled

When the option is not enabled, an `Attributes Changed` event is not recorded when an item that is created or copied has a Category Attribute applied to it, regardless of whether a user modifies the default value of the Category Attribute. An `Attributes Changed` event is recorded, however, if a user changes a Category Attribute value that is currently applied to an item from its existing value to a different one.

Table 18-1: Auditable Events

Event	Audit ID	Description
ActiveView Browse	2000210	Logged against a container object whenever an ActiveView template is used to render the browse view. This needs to be enabled in the Audit Interests Admin page and on the **Specific** tab of the ActiveView template itself.

Event	Audit ID	Description
Added to Package	302	An item was added to a Transport Package.
Added to Warehouse	300	An item was added to the Transport Warehouse.
Apply License	355	A license file was applied to Content Server or to a Content Server module.
Attachment Added	383	An attachment was added to a comment or to a reply.
Attachment Removed	384	An existing attachment was removed from a comment or from a reply.
Attributes Changed	10	One or more attributes of an item were changed.
Category Added	35	A Category was added to an item.
Category Removed	34	A Category was removed from an item.
Category Upgraded	409	An item with a Category had a newer version of the Category applied to it.
CD Ordered	22	A compound document was ordered or created.
Classification Applied	264	Classification was added to a managed item.
Classification Removed	265	Classification was removed from a managed item.
Classify Existing Content	199	Intelligent Classifications were assigned to all eligible managed objects.
Comment Created	373	A comment was added to a content message or to a content item.
Comment Deleted	375	An existing comment was deleted from a content message or from a content item.
Comment Edited	374	An existing comment was modified.
Configuration Changed	28	A Content Server configuration setting changed.
Content Moved	336	An item or item version was moved to a different Storage Provider.
Content Sharing - OpenText Core Audit History	2000802	A user stopped sharing an item and its OpenText Core audit details were collected.
Content Sharing - Released Share	2000803	A user with administrative permissions removed the shared lock on an item.
Content Sharing - Shared with OpenText Core	2000800	A user shared an item to OpenText Core
Content Sharing - Stopped Sharing with OpenText Core	2000801	A user stopped sharing an item.
Copy	4	An item was copied from one location to another.
Create	1	An item was created.

Event	Audit ID	Description
Create Node Split Transaction Rollback Error	343	Content Server failed to roll back a split transaction. A split transaction is a transaction that creates an item, and then adds a version to the item. If the second operation (adding a version) fails, Content Server rolls back the split transaction.
Custom Audit Event	2000586	A WebReports custom audit event was recorded. Enabling this interest enables the use of the WebReports `AUDITACTION` tag, which can be used by a WebReports developer to generate custom audit events. For more information on the `AUDITACTION` tag, see *OpenText Content Server - WebReports (LLESWEBR-UGD)*.
Data Source Purged	211	A data source was purged.
Database Maintenance	356	
Delete	2	An item was deleted.
Deployed from Warehouse	301	An item was deployed from the Transport Warehouse.
Edit	25	An item was edited.
eLink AutoSubscriptions Changed	169	An eLink item and its auto-subscription changed.
eLink Disabled	166	eLink was systematically disabled.
eLink Enabled	165	eLink was systematically enabled.
eLink Option Changed	188	The eLink attachment option changed.
eLink Sent Document Copy	220	eLink sent a copy of a document.
eLink Sent Document Link	221	eLink sent a link to a document.
eLink Subscribed	167	An item was eLink-subscribed.
eLink Unsubscribed	168	An item was eLink-unsubscribed.
Email Metadata Changed	402	Metadata for an Email item was updated. This can be caused by running the Email Metadata Utility, or by running a command from the **Maintain Email Metadata** administration page.
Enterprise Connect – Added from eDOCS	256	
Enterprise Connect – Log-in		
Enterprise Connect – Version Supersede	255	
Enterprise Database Re-Extracted	210	The database was re-extracted.
Failed Log-In Attempt	29	A logon attempt failed.
Function Executed	31	A Content Server function was executed.
Generation Created	15	A generation of an item was created.

Event	Audit ID	Description
Hit Highlight	254	A user applied Hit Highlighting to an item within a Search Results list.
Invalid Session Blocked	6543	The session of an externally-authenticated user became invalid.
LiveReport Executed	234	A LiveReport was executed.
Log-in	23	A user logged in to Content Server.
Log-in Disabled	6544	After repeated failed login attempts, a user account was disabled.
Log-out	24	A user logged off Content Server.
Major/Minor Disabled	42	Advanced (major/minor) versioning was disabled.
Major/Minor Enabled	41	Advanced (major/minor) versioning was enabled.
Members Changed	33	A user or group was added to, or removed from, a group. (The audit message is from the point of view of the user or group that was added or removed. For example, `User1 was removed from GroupA`.)
Membership Changed	30	A user or group was added to, or removed from, a group. (The audit message is from the point of view of the group that was added to or removed from. For example, `GroupA had User1 removed`.)
Move	3	An item was moved from one location to another.
Owner Changed	27	The ownership of an item changed.
Physical Objects – Assign Transfer	154	Transfer was assigned to physical item.
Permissions Changed	9	The permissions of an item changed.
Print	636003	One or more items was printed using Multi-File Output.
Project Membership Changed	32	A user or group was added to, or removed from, a project.
Provider Changed	37	An item's Storage Provider changed.
Provider Retry Delete Error Ignored	335	After an unsuccessful attempt to delete an item, a subsequent attempt was unsuccessful. See "Administering Blob Deletion Failures" on page 317.
Provider Retry Deleted	225	After an unsuccessful attempt to delete an item, a subsequent attempt was successful. For more information on `Provider Retry` events, see "Administering Blob Deletion Failures" on page 317.
Provider Retry Queued	222	After an unsuccessful attempt to delete an item, the deletion retry was queued. See "Administering Blob Deletion Failures" on page 317.
Provider Retry Queuing Error	224	After an unsuccessful attempt to delete an item, the queuing of the deletion retry resulted in an error. See "Administering Blob Deletion Failures" on page 317.

Event	Audit ID	Description
Provider Retry Retried	223	After an unsuccessful attempt to delete an item, the deletion was attempted again. See “Administering Blob Deletion Failures“ on page 317.
Purge	13	An item was automatically purged from the Recycle Bin. See “Configuring Recycle Bin” on page 408.
Purge Collections Items Audit Records	351	A system administrator manually deleted records pertaining to operations performed on one or more Collections. See *OpenText Content Server - Administering Collections (LLESCL-AGD)*.
Purge now	391	A user manually purged an item in the Recycle Bin by selecting it and clicking **Purge**. See “Restoring and Purging Deleted Items” on page 406.
Recovery Failure	209	The content of an item could not be accessed during extraction to the search index, (so the item’s content is not searchable). The item was placed in the recovery state. Content Server makes additional attempts to extract the content of items that are in the recovery state.
Recovery Success	208	After a Recovery Failure event occurred and an item was placed in the recovery state, Content Server successfully extracted the item’s content to the search index.
Release Created	20	A release of a compound document was created.
Release Deleted	21	A release of a compound document was deleted.
Rename	5	An item was renamed.
Rendition Created	16	A rendition of an item was created.
Rendition Deleted	17	A rendition of an item was deleted.
Reply Created	378	A reply was added to a comment on a content message or to a comment on a content item.
Reply Deleted	380	An existing reply was deleted.
Reply Edited	379	An existing reply was modified.
Reserve	6	An item was reserved.
Restore	46	A deleted item was restored.
Revision Created	18	A revision of a compound document was created.
Revision Deleted	19	A revision of a compound document was deleted.
Saved Query Changed	341	A Search Form, Slice, or saved query was changed.
Saved Query Created	340	A Search Form, Slice, or saved query was created.
Saved Query Executed	342	A Search Form, Slice, or saved query was run.
Search Agent Disabled	369	A configured search agent for Prospectors or Classifications was disabled.

Event	Audit ID	Description
Search Agent Enabled	368	A configured search agent for Prospectors or Classifications was enabled.
Search Statistics Auto-Purged	218	Search statistics were automatically purged.
Security Clearance – Clearance Level Changed	164	Security clearance level was changed
Search Statistics Purged	217	Search statistics were purged.
Shortcut Added	385	A shortcut to an item was added to a comment or to a reply.
Shortcut Created	8	A shortcut to an item was created.
Shortcut Removed	372	A shortcut to an item was removed from a comment or from a reply.
Thumbnail Created	352	A thumbnail image of a Content Server item was created.
Thumbnail Deleted	353	A thumbnail image of a Content Server item was deleted.
Thumbnails Deleted All	354	All of the thumbnail images of a Content Server item were deleted.
Unreserve	7	An item was unreserved.
Version Added	11	A version was added to an item.
Version Control Changed	44	The version control changed.
Version Deleted	12	A version was deleted.
Version Locked	39	An item version was locked.
Version Opened	14	An item version was opened.
Version Promoted	43	A document item was promoted from a minor version to a major version.
Version Superseded	228	Content Server replaced a version of a document edited using WebDAV with a more recent document version. This event occurs when the `Enable collapse versions within a single editing session` settings is enabled and a document is saved multiple times during a single editing session. For more information, see *OpenText WebDAV - Administering WebDAV (LLESWDV-AGD)*.
Version Unlocked	40	An item version was unlocked.
View	26	An item was viewed.
WebReports Export to Client	2000208	A WebReport was executed with a destination of `Browser`.
WebReports Export to Desktop	2000201	A WebReport was executed with a destination of `Desktop`.
WebReports Export to email	2000202	A WebReport was executed with a destination of `Email`.
WebReports Export to Form	2000207	A WebReport was executed with a destination of `Form`.

Event	Audit ID	Description
WebReports Export to FTP Server	2000585	A WebReport was executed with a destination of `FTP Server`.
WebReports Export to Node	2000203	A WebReport was executed with a destination of `Content Server Node`, which creates a new Content Server item.
WebReports Export to Node Version	2000205	A WebReport was executed with a destination of `Content Server Version`, which adds a version to a Content Server item.
WebReports Export to Server	2000204	A WebReport was executed with a destination of `Server`. The `Server` destination allows the WebReport output to be sent to a location on the server where Content Server is running, for example, `C:/WRoutput/myOutputFile.csv`.
WebReports Run	2000209	A WebReport was executed. `WebReports Run` is a generic event that is logged whenever a WebReport is run, regardless of its destination.
WebReports Workflow	2000206	A WebReport was executed with a destination of `Worklow`, which initiates a Workflow.
Workflow Status Changed	170	The status (suspended, executing, stopped, archived, or deleted) of an executing workflow changed.
Xml Export	233	An XML export action was performed on an item.
Zip and Download	636002	An item or series of items was zipped and downloaded using Multi File Output.
Zip and Email	636001	An item or series of items was zipped and emailed using Multi-File Output.

18.1.1 To Set Auditing Interests

To set auditing interests:

1. Click the **Administer Event Auditing** link in the **System Administration** section of the Administration page.

2. On the **Administer Event Auditing** page, click **Set Auditing Interests**.

3. On the **Set Auditing Interests** page, in the **Events** section, to add an event type that you want audited, select that event type's check box.

   To stop auditing an event type, clear that event type's check box.

4. Optional In the **Options** section, if you want to enable the auditing of any auditable actions performed by users with the System Administration privilege, select **Force auditing of all events performed by System Administrators**.

5. Click **Set Interests**.

6. Click the **Admin Home** link to return to the Administration page.

18.1.2 To View All Currently Set Auditing Interests

To view all currently set auditing interests:

1. Click the **Administer Event Auditing** link in the **System Administration** section on the Administration page.
2. On the **Administer Event Auditing** page, click **Set Auditing Interests**.

18.2 Viewing and Managing Audit Records

To view specific Content Server audit log entries, query the audit log. Query results are returned on the the **Audit Query Results** page.

The **Audit Query Results** page lists all of the audited events and items that match the criteria you specified on the **Query Audit Log** page. You can change the criteria by clicking the **Back to Query Page** button ⇦ and modifying the information.

Tip: To view other result pages, click the **Previous** or **More** buttons at the bottom of the result list. To return to the Administration page, click the **Admin Home** link.

The following tables list values that are associated with the events on the **Audit Query Results** page.

Permission Name	Decimal Value	Hex	Bits
See Only	130	0x82	8, 2
See Contents Only	36865	0x9001	16, 13, 1
Modify Only	65536	0x10000	17
Edit Attributes Only	131072	0x20000	18
Add Items Only	4	0x4	3
Delete Versions Only	16384	0x4000	15
Delete Only	8	0x8	4
Reserve Only	8192	0x2000	14
Edit Permissions Only	16	0x10	5
See Contents Perm	36995	0x9083	16, 13, 8, 2, 1
Modify Perm	65666	0x10082	17, 8, 2
Edit Attributes Perm	233603	0x39083	18, 17, 16, 13, 8, 2, 1
Add Items Perm	65670	0x10086	17, 8, 3, 2
Delete Versions Perm	118915	0x1D083	17, 16, 15, 13, 8, 2, 1

Permission Name	Decimal Value	Hex	Bits
Delete Perm	118923	0x1D08B	17, 16, 15, 13, 8, 4, 2, 1
Reserve Perm	110723	0x1B083	17, 16, 14, 13, 8, 2, 1
Edit Permissions Perm	258207	0x3F09F	18, 17, 16, 15, 14, 13, 8, 5, 4, 3, 2, 1

RightID	Privileges
1	Owner
2	Group
3	Public Access
4	System (deprecated)

Audit log information is stored in tables in the Content Server database. You can increase your database storage capacity by periodically purging unnecessary data. You can purge the audit log based on date, user, and event type. When you purge the audit log, Content Server removes rows from the `DAuditNew` table in the Content Server database. If corresponding rows exist in the `DAuditMore` table, they are also removed.

Warning

The purge action cannot be undone. To ensure that you purge the proper items or events, you should query the audit log to display the items or events that you intend to purge prior to purging any items.

After you set the auditing interests, you can consult the audit logs to monitor database usage and diagnose problems. Content Server users can view the audit log for single items by clicking its **Functions** icon ▾, choosing **Info**, and then choosing **Audit**.

18.2.1 To Query the Audit Log

To query the audit log:

1. Click **Query Audit Log** in the **System Administration** section of the Administration page.
2. In the **Target Items** section, do one of the following:
   - To view the audit log for all items, click the **All** radio button.
   - To view the audit log for a specific type of item, click the **By Type** radio button, and then select an item type from the list.

     Note: Selecting **User or Group** will return results for the following item types: User, Group, X-Domain Group, and Factory.

- To view the audit log for a single item, click **Single Item**. Click the **Browse Content Server** button, navigate to the item, and then click its **Select** link.
- To view the audit log of events performed on a user or group, click **Single User/Group**, and then find a user or group.

3. Click the type of event for which you want the audit results displayed in the **Event Type** list.

   Tip: Click **<Any>** to view results for all event types.

4. In the **Performers** section, do one of the following:

   - To view the audit log of events performed by any user and group, click **All**.
   - To view the audit log of events performed by a specific user, click **Specific User**, and then select a user or group.

5. Click a month, day, and year in the **From Date** and **To Date** lists to specify an inclusive time frame by which to search.
6. Click a value in the **Rows Per Page** list to specify the number of items that appear on a page.
7. Click **Submit Query**.

Note: A broad query can potentially return a large number results, depending on the size of the database. OpenText recommends that you restrict the results by specifying an item type, event type, user, and/or date range. Also, impossible combinations will return zero results. For example, if you select **Folder** as the item type and **Add Version** as the event type, the query will not return any results.

18.2.2 To Purge the Audit Log

To purge the audit log:

1. In the **System Administration** section of the Administration page, click the **Administer Event Auditing** link.
2. On the **Administer Event Auditing** page, click the **Purge Audit Log** link.
3. In the **Target Items** section, do one of the following:

   - To purge all items, click the **All** button.
   - To purge specific items, click the **By Type** button, and then select the type you want to purge from the list.

     Note: Selecting **User** or **Group** will automatically purge the following item types: User, Group, X-Domain Group, and Factory.

- To purge a single item, click the **Single Item** button, and then click the **Browse Content Server** button, navigate to the item you want to purge, and then click its **Select** link.
- To purge items that belong to a specific user or group, click the **Single User/ Group** radio button, and then find a user or group.

4. To purge the audit log of a specific type of event, select the event from the **Event Type** list.

   Tip: To purge the audit log of all event types, click **<All>**.

5. In the **Performers** section, do one of the following:

   - To purge the audit log of all users and groups, click the **All** button.
   - To purge the audit log of a specific user, click the **Specific User** button, and then find a user or group.

6. To purge the audit log of items or events within a specific time frame, click a month, day, and year from the **From Date** and **To Date** calendars.
7. Click **Purge**.
8. Click the **Admin Home** link to return to the Administration page.

18.2.3 To Manage Audit Records Created in Prior Releases

Note: You can manage audit records created in prior releases after you upgrade a database from a previous version of Content Server.

To manage audit records created in prior releases:

1. On the Content Server Administration page, in the **System Administration** section, click **Administer Event Auditing**.
2. On the **Administer Event Auditing** page, click **Manage Audit Records Created in Prior Releases**.

   Note: Clicking either of the following options may be time consuming. Once you have made your selection, you will see a progress page. Wait until the progress page updates itself, then click **Admin home**.

3. On the **Manage Audit Records Created in Prior Releases** page, do one of the following:

   - To convert audit records from previous releases of Content Server, click **Convert Audit Records Created in Prior Releases**.
   - To remove audit records created in previous releases of Content Server, click **Purge Audit Records Created in Prior Releases**.

18.3 Managing Audit Security Settings

To protect the accuracy and integrity of the Content Server audit log, ordinary users cannot access the Content Server audit log administrative functions. To query the audit log, you must have the `Query Audit Log` usage privilege. To set auditing interests and purge the audit log, you must have the `System administration rights` privilege and the Web Admin usage privilege. To further restrict access to the audit log and its settings, you can enable Audit Security Settings.

Tip: You may wish to enable audit security settings if your organization is regulated and it is mandatory that you can demonstrate the integrity of the audit log.

Content Server Audit Security Settings allow for several levels of increased restriction:

Tip: If you enable any of these security levels, users can query the audit log, but cannot add or remove auditing interests or purge the audit log.

For more information about the auditing interests page, see “Managing Audit Interests” on page 320. For more information about the audit log, see “Viewing and Managing Audit Records” on page 327.

- You can configure Content Server so that only the Admin user can set auditing interests and purge the audit log.
- You can configure Content Server so that *no user at all* can purge the audit log.
- You can configure Content Server so that *no user at all* can make changes to your audit interests configuration.

Important

Consider carefully before you decide to prevent purging of the audit log or changing the audit interests. Once you take either of these steps, they cannot be disabled. For example, if you prevent changes to your audit interests configuration, you will be unable to enable new auditing interests added by a new Content Server module, or disable such new auditing interests that are enabled by default.

18.3.1 To Configure Audit Security Settings

To configure audit security settings:

1. Log on to Content Server as the Admin user.

   Note: You must be logged on as Admin to configure audit security settings. You cannot configure audit security settings logged on as any other user, regardless of your rights and usage privileges.

2. In the **System Administration** section of the Administration page, click **Administer Event Auditing**.

3. On the **Administer Event Auditing** page, click **Audit Security Settings**.

4. On the **Audit Security Settings** page:

   a. Optional If you want to prevent any user other than the Admin user from purging the audit log or modifying your audit interests, enable **Limit Audit Config to "Admin" User**.

   b. Optional If you want to prevent any user at all from purging the audit log:

      i. To prevent any user, including the Admin user, from purging the audit log, click **Disable Audit Purge**.

         Important
         Clicking **Disable Audit Purge** cannot be undone. If the audit log becomes large, you may see an impact to performance.

         Tip: The **Disable Audit Purge** button is disabled if audit purge has already been disabled.

      ii. In the **Disable Audit Purge?** dialog box, enable **I understand the risk involved by enabling this setting and want to continue**, and then click **OK**.

   c. Optional If you want to prevent any user at all from changing the audit interests configuration:

      i. To prevent any user, including the Admin user, from modifying the auditing interests and ensuring that the **Set Auditing Interests** page becomes read-only, click **Lock Audit Interests**.

         Important
         Clicking **Lock Audit Interests** cannot be undone. In the event that new interests are added to Content Server, for example if you install a new module or upgrade an existing module, those new interests cannot be audited.

         Tip: The **Lock Audit Interests** button is disabled if auditing interests have already been locked.

   ii. In the **Lock Audit Interests?** dialog box, enable **I understand the risk involved by enabling this setting and want to continue**, and then click **OK**.

d. Click **Submit**.

Chapter 19

Administering Item Control

On the **Administer Item Control** page, you can enable and configure settings that determine the default behavior of Content Server items that are reservable or versionable. Specifically, you can:

- Set the maximum number of versions that Content Server will keep for any item by setting a “Version Limit” on page 335.
- Configure how you “Reserve” on page 335 a Document so that:
  - Groups can reserve and unreserve Documents
  - The **Add New Version** option is selected by default when users unreserve a Document
- Enable “Advanced Version Control” on page 336 for Documents so that Content Server items can use a versioning scheme that includes both major and minor versions. When a Document uses advanced versioning, Document authors can be given permission to access minor (draft) versions of Documents, while other users can be restricted to viewing only the major (published) versions of Documents.
- Encourage or require users to complete Category information when they add a Document by enabling the “Advanced Add Item” on page 337 process.
- Disable “Table Key Lookup Validation” on page 338 to improve performance in a test environment.

Version Limit

By default, Content Server allows users to create an unlimited number of versions of each item. To restrict the number of versions that users are allowed to create, you can set a version limit. If an item has reached its version limit, Content Server purges the oldest version of an item when a user adds a new version.

Reserve

Group Reserve Capability

By default, only users can reserve Content Server items. To allow groups to reserve and unreserve Content Server items, enable **Group Reserve Capability**. This allows users to select from a list of groups when they reserve an item. Any group member who has sufficient permissions (**Reserve** access) can unreserve an item that has been reserved by a group.

Unreserve Document

Select **Enable “Add New Version” by default** to have Content Server enable the **Add New Version** option when it displays the **Unreserve: <*Document*>** page to a user.

Tips

- If **Enable "Add New Version" by default** is not selected, the **Add New Version** option still appears on the **Unreserve:** <*Document*> page, but it is not enabled by default.
- Selecting **Enable "Add New Version" by default** does not prevent users from clearing the **Add New Version** option on the **Unreserve:** <*Document*> page.

Advanced Version Control

Advanced Version Control

By default, **Advanced Version Control** is enabled. Content Server users can specify that a Document will use **Standard** (linear) or **Advanced** (major/minor) versioning when they create a Document. You can disable **Advanced Version Control** if you don't want users to have the option of using advanced versioning.

Advanced Version Type

Choose between **Classic Advanced Versioning** and **Enhanced Advanced Versioning**. By default, **Classic Advanced Versioning** is enabled.

Classic Advanced Versioning

In **Classic Advanced Versioning**, the Content Server Browse View displays the metadata (such as the size and MIME type) of a Document's latest major version, and the commands on a Document's **Functions** menu act on the latest major version of the Document. This is true even if the latest version of the Document is a minor version and the current user has access to minor versions of the Document.

In **Classic Advanced Versioning**, users must open a Document's **Versions** Properties page to promote one of its minor versions to a major version or to perform other operations on them.

Classic Advanced Versioning is the only Advanced Version Type available in Content Server 16.2.3 and earlier.

Note: If you use Classic Advanced Versioning and you want to expose Document version information in the Content Server interface as a custom column, you should select the **Version** data source. The behavior of the **Version** data source corresponds to the behavior of Classic Advanced Versioning. For example, it displays the latest major version of a Document, even if a minor version exists and current user has permission to access it.

Enhanced Advanced Versioning

In **Enhanced Advanced Versioning**, Content Server displays the Document metadata and the **Functions** menu commands that are appropriate for the current user. Users that open, edit, or download a Document are shown the latest minor or major version that they have permission to work with.

Tip: This means that different users may see different things when they click the same item. For example, a user who has access to minor Document versions could send a link to a user who does not, and the recipient would see the latest major Version of the Document, or even no Document at all (if only minor Versions of the Document exist).

Similarly, if **Enhanced Advanced Versioning** is enabled, a Document's **Functions** menu reflects the permissions that the current user has. For example, a user that has access to minor Document versions can see a **Promote to Major** command in a Document's **Functions** menu, whereas a user that has access only to major Document versions will not.

When **Enhanced Advanced Versioning** is enabled, users typically do not need to open a Document's **Versions** page to work with minor Document versions.

Note: If you use Enhanced Advanced Versioning and you want to expose Document version information in the Content Server interface as a custom column, you should select the **Advanced Version** data source. The behavior of the Advanced Version data source corresponds to the behavior of Enhanced Advanced Versioning. For example, it displays the latest minor or major version of a Document that the current user has permission to access.

Major Version Only Access

When **Advanced Version Control** is enabled, the **Major Version Only Access** setting controls how Content Server displays items that use advanced versioning. If **Major Version Only Access** is enabled, Content Server does not display minor Document versions to users who do not have permission to access them. (To access a minor version of a Document, you require **Reserve** permission or greater). Such users see instead the latest major version of the Document.

Tip: If **Major Version Only Access** is enabled, Content Server does not display a Document that has only minor versions to users that do not have at least Reserve permission to the Document.

Advanced Add Item

The **Advanced Add Item** process works in tandem with the **Administer MIME Types and Categories** page, where you can associate a MIME type with one or more Categories. When the **Advanced Add Item** process is enabled, users who create a Document that has a MIME type associated with a Category are directed to a page where they can fill out the Document's Category Attributes. If the Document's MIME type is associated with multiple Categories, an initial page offers the user the choice of which Categories to apply to the Document. If a Category associated with a MIME type has required Attributes, users must specify values for the required Attributes before they can complete the **Advanced Add Item** process.

For more information, see "Associating MIME Types and Categories" on page 237. For general information about MIME type settings, see "Administering MIME Types and Icons" on page 233.

Table Key Lookup Validation

You can disable Table Key Lookup validation to improve performance in a test environment.

19.1 To Configure Item Control Parameters

To configure item control parameters:

1. In the **System Administration** section of the Content Server Administration page, click **Administer Item Control**.
2. On the **Administer Item Control** page, in the **Version Limit** section, type a numerical value in the **Set Version Limit Default Value** box to set the default maximum number of versions for Content Server items.

   Note: The default value for this field is `Unlimited`. To reset the Version limit to an unlimited value, type either `Unlimited` or `-1` in the **Set Version Limit Default Value** field.

3. In the **Reserve** section:

   a. Beside **Group Reserve Capability**, select **Show group list** to allow groups to reserve Content Server items.

   b. Beside **Unreserve Document**, select **Enable "Add New Version" by default** to automatically enable the **Add New Version** option on the **Unreserve** page.

4. In the **Advanced Version Control for Documents** section:

   a. Beside **Advanced Version Control**, select **Enable advanced major/minor versioning for Documents in the system** to allow users to specify whether a Document will use standard or advanced versioning when they create a Document.

   b. Beside **Advanced Version Type**, select **Classic Advanced Versioning** to show only major versions of Documents on a normal browse page or select **Enhanced Advanced Versioning** to display the latest minor or major version that a user has permission to see.

   c. Beside **Major Version Only Access**, select **For users with major Version only access, hide Documents that only have minor Versions** to hide minor versions of Documents from users who do not have permission to access them.

5. In the **Advanced Add Item** section, beside **Required Attributes**, select **Display categories on second Add Item page** to enable the two-step Advanced Add Item process.

6. In the **Table Key Lookup** section, beside **Validation**, select **Skip Validation for Text:Table Key Lookup attribute** to turn off validation to improve Content Server performance during testing or migration.

7. Click **Save Changes**.

Chapter 20

Administering Modified Date Triggers

The settings on this page determine whether the following events trigger an update to an item's **Modified** property.

- a change is made to the item's permissions (including changes to access rights, Owner, Owner Group, and Public Access)
- a change is made to the Categories or attributes applied to the item

By default they do. To prevent either setting from affecting an item's **Modified** property, disable it.

These settings affect all items throughout your Content Server deployment.

20.1 To Set Modification Date Triggers

To set modification date triggers:

1. Click **Administer Modified Date Triggers** in the **System Administration** section of the Content Server Administration page.
2. On the **Administer Modified Date Triggers** page, select the event types that will cause the **Modified** property of an item to be updated.
3. Click **Save Changes**.

Chapter 21

Administering Object Privileges and Usage Privileges

A Content Server administrator manages Object and Usage Privileges to protect Content Server data and system integrity:

- Object Privileges grant users and groups the ability to create certain types of Content Server items
- Usage Privileges grant users and groups the ability to perform certain types of Content Server tasks

21.1 Managing Object Privileges

Content Server Object Privileges regulate the ability of users to create certain Content Server items.

By default, all Content Server objects, except Category, LiveReport, URL, and Custom View and Appearance object types, are *unrestricted*, which means that users and groups have the necessary privileges to create the item types in Content Server. Only the Admin user initially has the privileges necessary to create LiveReports, URLs, and Custom Views. These settings can be changed by restricting or unrestricting the object type for specific groups or users.

A user who has the item creation privilege for LiveReports can issue SQL statements to the RDBMS, including statements that can alter the Content Server database. To maintain the integrity of your Content Server database, OpenText recommends that you restrict the LiveReports creation privilege to the Admin user or to only a small number of users who are knowledgeable about SQL and the Content Server schema. To protect your database, the Modify permission for LiveReports requires that a Content Server user have the LiveReport item creation privilege.

Note: Optional installed modules have their own default settings and restrictions. Optional modules may restrict object and usage privileges by default.

21.1.1 Restricting Object Privileges

To restrict object privileges:

1. Click **Administer Object Privileges** in the **System Administration** section of the Content Server Administration page.
2. On the **Administer Object Privileges** page, click **Restrict** beside the object type whose privilege you wish to restrict.
3. Click **OK** in the confirmation dialog box that appears.
4. Search for the users or groups to whom you want to grant the object privilege, and then enable **Add to group** beside the group or user name.
5. Click **Submit**.
6. When you are done selecting users and groups, click **Done**.

21.1.2 Modifying Object Privileges

To modify object privileges:

1. Click **Administer Object Privileges** in the **System Administration** section of the Content Server Administration page.
2. On the **Administer Object Privileges** page, click **Edit Restrictions** beside the object type whose privilege you wish to modify.
3. To grant the privilege to new users or groups, search for the users or groups to whom you want to grant the object privilege, enable **Add to group** beside the group or user name, and then click **Submit**.

   To remove the privilege from existing users or groups, click the name of the user or group on the left, and then click **Remove From Group** on the right.
4. When you have finished making modifications, click **Done**.

21.2 Managing Usage Privileges

Content Server usage privileges regulate a user’s ability to perform certain Content Server actions.

For example, users who require access to the Content Server Administration pages must have both the System Administration and Web Admin privileges. As a Content Server administrator, you can assign the **Web Admin** usage privilege, and other usage privileges, on the **Administer Usage Privileges** administration page

Usage privileges are either restricted or unrestricted by default. If a usage privilege is unrestricted, any user can perform the action enabled by the privilege. If a usage privilege is restricted, only users and groups that you add to the usage privilege can perform the action. (This applies to Content Server administrators too. Administrators do not have access to restricted usage privileges unless they are added.) Optionally, you can delete all restrictions to set the **Usage Status** to unrestricted, so that all users and groups can perform the action enabled by the usage privilege.

This section of the Admin Help describes the usage privileges that are present after you perform a basic installation of Content Server. (Optional modules may introduce additional usage privileges.) For each usage privilege, this section tells you whether the usage privilege is restricted by default, what the usage privilege enables a user to do, and suggests reasons that you may choose to restrict the usage privilege. The suggested reason to restrict can be one or more of the following:

Performance
The usage privilege may allow a user to perform actions that place a high load on the Content Server computer or database.

Security
The usage privilege may elevate the user's access permissions and possibly provide unauthorized access to items or Content Server metadata.

User Experience

- Restricting the usage privilege may simplify a user's options by hiding options that a user is not likely to perform.
- Restricting the usage privilege may prevent a user from inadvertently performing an unexpected action.
- Restricting the usage privilege to a group of knowledgeable and trustworthy users may help to protect system integrity.

Tip: The **Administer Usage Privileges** page lists usage privileges by usage type and usage name. Similarly, this section groups usage privileges by usage type. So, for example, to obtain information on the **Copy Items to Another Collection** usage privilege, refer to the "Collections Command and Collections Operation Usage Privileges" on page 357 section.

For usage types that have only a single privilege, the description of the usage privilege can be found in "Other Usage Privileges" on page 368. So, for example, to obtain information on the **Set Best Bets Values** usage privilege, look in "Other Usage Privileges" on page 368, because **Set Best Bets Values** is the only usage privilege that falls under the **Best Bets Administration** usage type.

Restricting Usage Privileges

To restrict usage privileges:

1. Click **Administer Usage Privileges** in the **System Administration** section of the Content Server Administration page.
2. On the **Administer Usage Privileges** page, click **Restrict** beside the usage type whose privilege you wish to restrict.

3. Click **OK** in the confirmation dialog box that appears.

4. Search for the users or groups to whom you want to grant the usage privilege, and then enable **Add to group** beside the group or user name.

5. Click **Submit**.

6. When you are done selecting users and groups, click **Done**.

Modifying Usage Privileges

To modify usage privileges:

1. Click **Administer Usage Privileges** in the **System Administration** section of the Content Server Administration page.

2. On the **Administer Usage Privileges** page, click **Edit Restrictions** beside the usage privilege that you wish to modify.

3. To grant the privilege to new users or groups, search for the users or groups to whom you want to grant the usage privilege, enable **Add to group** beside the group or user name, and then click **Submit**.

   To remove the privilege from existing users or groups, click the name of the user or group on the left, and then click **Remove From Group** on the right.

4. When you have finished making modifications, click **Done**.

21.2.1 ActiveView Usage Privileges

ActiveView usage privileges regulate the ability of users to perform activities related to ActiveView and Perspectives. For more information, see:

- *OpenText Content Server - ActiveView (LLESAV-UGD)*
- *OpenText Content Server - ActiveView (LLESAV-UGD)*
- *OpenText Content Server - ActiveView (LLESAV-UGD)*

Table 21-1:

Usage Type	Usage Name	Default Setting	Reason to Restrict	Effect
ActiveView	ActiveView Tab	Restricted	security, user experience	Allows you to view and manage ActiveView overrides for the Classic View of the Content Server user interface.

Usage Type	Usage Name	Default Setting	Reason to Restrict	Effect
ActiveView	ActiveView Usage Tab	Restricted	security, user experience	Allows you to see a list of which nodes are affected by the current ActiveView template.
ActiveView	Perspectives Tab	Restricted	security, user experience	Allows you to view and manage ActiveView overrides for the Smart View of the Content Server user interface.

21.2.2 Business Administration Usage Privileges

Business Administration usage privileges enable Content Server users to access specific sections of the Content Server Administration page and to perform a limited set of administrative duties. In general, the administrative abilities enabled by Business Administration usage privileges affect the appearance and behavior of Content Server, do not require Content Server to be restarted, and have low performance impacts. After you assign one or more Business Administration usage privileges to a user, that user can act as an administrator in specific areas.

Note: Users with Business Administration usage privileges do not require the Web Admin usage privilege. A user with any Business Administration privilege sees an Admin menu and can access the Content Server Administration page without being assigned any additional usage privilege.

To enable a user or group to perform any task enabled by a Business Administration usage privilege, assign the Business Administration usage privileges globally. Alternatively, to enable a user or group to perform a limited set of administrative duties in a specific area, assign only the specific Business Administration usage privilege that they require.

Assigning Business Administration Usage Privileges Globally

By default, Content Server creates a group named **Business Administrators** that is assigned to each of the Business Administration usage privileges. Initially, the only member of the **Business Administrators** group is the Admin user. To grant a user or group access to all of the Business Administration tasks, add the user or group to the **Business Administrators** group.

Note: When Content Server is upgraded, if there is already a group named **Business Administrators**, Content Server instead creates a group named

Business Administrators-1, and assigns it to each of the Business Administration privileges.

Assigning Business Administration Usage Privileges Individually

Business Administration usage privileges can be assigned individually in the same way that other usage privileges are assigned. For more information, see "Managing Usage Privileges" on page 344.

Example: To enable a Content Server user to act as an administrative resource to a team that works on Facets and Columns, assign the**Facets and Columns** Business Administration privilege. To assign the user all of the Business Administration usage privileges at once, add the user to the **Business Administrators** group. In the latter case, the user will be able to do Facets and Columns work, and numerous other administrative duties too.

Table 21-2: Content Server Business Administration Usage Privileges

Usage Type	Usage Name	Default Setting	Reason to Restrict	Effect
Business Administration	Available Features	Restricted	User Experience	See "The Available Features Usage Privilege" on page 349.
Business Administration	Classic Interface Configuration	Restricted	User Experience	See "The Classic Interface Configuration Usage Privilege" on page 350.
Business Administration	Data Policies	Restricted	User Experience	See "The Data Policies Usage Privilege" on page 352.
Business Administration	Facets and Column	Restricted	User Experience	See "The Facets and Columns Usage Privilege" on page 354.
Business Administration	Query Audit Log	Restricted	User Experience	See "The Query Audit Log Usage Privilege" on page 355.
Business Administration	Recycle Bin Configuration	Restricted	User Experience	See "The Recycle Bin Configuration Usage Privilege" on page 355.

Usage Type	Usage Name	Default Setting	Reason to Restrict	Effect
Business Administration	Reminder Configuration	Restricted	User Experience	See "The Reminder Administration Usage Privilege" on page 356.
Business Administration	User and Group Configuration	Restricted	User Experience	See "The User and Group Configuration Usage Privilege" on page 356.

The Available Features Usage Privilege

The **Available Features** Business Administration usage privilege enables access to the following administration pages:

Configure Container Options

The **Configure Container Options** page allows you to specify the way users browse containers in Content Server, to enable pagination, filtering and column customization, to set the behavior of Featured Items and Custom Views, and to enable Drag and Drop.

To open the **Configure Container Options** page from the Content Server Administration page, click **Configure Features** in the **Server Configuration** section, and then click **Configure Container Options**.

For more information on the **Configure Container Options** page, see "Configuring Container Options" on page 22.

Configure Thumbnail Options

The **Configure Thumbnail Options** page allows you to specify whether thumbnails are generated when Content Server indexes documents in an Enterprise Data Source, and to configure settings relate to Thumbnail generation, such as the MIME types that are enabled for Thumbnail generation.

To open the **Configure Thumbnail Options** page from the Content Server Administration page, click **Configure Features** in the **Server Configuration** section, and then click **Configure Thumbnails**.

For more information on the **Configure Thumbnail Options** page, see "Configuring Thumbnail Options" on page 28.

Configure Best Bets Settings

The **Configure Best Bets Settings** page allows you to define or change how Best Bets results are displayed, and the number of results to display, on the Search Results page.

To open the **Configure Best Bets Settings** page from the Content Server Administration page, click **Configure Best Bets Settings** in the **Best Bets Administration** section.

For more information on the **Configure Best Bets Settings** page, see *OpenText Content Server - Administering Search (LLESWBS-AGD)*.

Configure Search Location Modifiers

The **Configure Search Location Modifiers** page allows you to to extend a search from the current Content Server location to also search within folders and subfolders that are linked from the current folder as shortcuts.

To open the **Configure Search Location Modifiers** page from the Content Server Administration page, click **Configure Search Location Modifiers** in the **Search Administration** section.

For more information on the **Configure Search Location Modifiers** page, see *OpenText Content Server - Administering Search (LLESWBS-AGD)*.

The Classic Interface Configuration Usage Privilege

The **Classic Interface Configuration** Business Administration usage privilege enables access to the following administration pages:

Configure Functions Menu

The **Configure Functions Menu** page allows you to determine where functions appear on a Content Server item's **Functions** menu.

To open the **Configure Functions Menu** page from the Content Server Administration page, click **Configure Functions Menu** in the **Server Configuration** section.

For more information on the **Configure Functions Menu** page, see "Configuring the Functions Menu" on page 32.

Configure Document Functions

The **Configure Document Functions** page allows you to enable and disable the **Open** and **View as Web Page** functions in Content Server and the Document Overview page.

To open the **Configure Document Functions** page from the Content Server Administration page, click **Configure Presentation** in the **Server Configuration** section, and then click **Configure Document Functions**.

For more information on the **Configure Document Functions** page, see "Configuring Document Functions" on page 38.

Configure Promoted Functions

The **Configure Promoted Functions** page allows you to make certain document-management functions easier to find in the user interface by promoting them. Promoted functions are displayed more prominently for Documents on the **Detail View** page of containers and Workspaces, and the **View as Web Page** and **Properties** pages for Documents.

To open the **Configure Promoted Functions** page from the Content Server Administration page, click **Configure Presentation** in the **Server Configuration** section, and then click **Configure Promoted Functions**.

For more information on the **Configure Promoted Functions** page, see "Configuring Promoted Functions" on page 39.

Configure Sidebar

The **Configure Sidebar** page allows you to enable or disable the **Content Filter** sidebar and sidebar panels.

To open the **Configure Sidebar** page from the Content Server Administration page, click **Configure Presentation** in the **Server Configuration** section, and then click **Configure Sidebar**.

For more information on the **Configure Sidebar** page, see "Configuring the Sidebar" on page 40.

Configure Small and Large Icon Views

The **Configure Small and Large Icon Views** page allows you to enable or disable small and large icon views in the user interface. When the **Display Large and Small Icon Views** setting is enabled, containers can display items using the Detail, Large, and Small Icon Views and users can enable whichever view they like.

To open the **Configure Small and Large Icon Views** page from the Content Server Administration page, click **Configure Presentation** in the **Server Configuration** section, and then click **Configure Small and Large Icon Views**.

For more information on the **Configure Small and Large Icon Views** page, see "Configuring Small and Large Icon Views" on page 41.

Project Settings

The **Project Settings** page allows you to configure the default appearance and behavior of Content Server Projects. To open the **Project Settings** page from the Content Server Administration page, click **Configure Presentation** in the **Server Configuration** section, and then click **Project Settings**.

For more information on the **Project Settings** page, see "Configuring Project Presentation Settings" on page 42.

Configure System Messages

The **Configure System Messages** page allows you to broadcast information to all users on the system using the News Player.

To open the **Configure System Messages** page from the Content Server Administration page, click **Configure System Messages** in the **Server Configuration** section.

For more information on the **Configure System Messages** page, see "Configuring System Messages" on page 47.

Configure Status Page for Multi-Select Actions

The **Configure Status Page for Multi-Select Actions** page enables Content Server to show a status page that shows the progress of items that are in the process of being copied, moved, or deleted.

To open the **Configure Status Page for Multi-Select Actions** page from the Content Server Administration page, click **Configure Status Page for Multi-Select Actions** in the **System Administration** section.

For more information on the **Configure Status Page for Multi-Select Actions** page, see "Configuring the Status Page for Multi-Select Actions" on page 373.

Configure Recommender Components

The **Configure Recommender Components** page allows you to configure the appearance of the Recommendations and Ratings pages.

To open the **Configure Recommender Components** page from the Content Server Administration page, click **Configure Recommender Components** in the **Recommender Administration** section.

For more information on the **Configure Recommender Components** page, see *OpenText Content Server Admin Online Help Collection - Recommender Administration (LLESREC-AGD)*.

Configure Required Search Results Fields

The **Configure Required Search Results Fields** page allows you to set specific search results fields as required so that these fields always appear on the Search Results page.

To open the **Configure Required Search Results Fields** page from the Content Server Administration page, click **Configure Required Search Results Fields** in the **Search Administration** section.

For more information on the **Configure Required Search Results Fields** page, see *OpenText Content Server - Administering Search (LLESWBS-AGD)*.

Configure Department Selection

The **Configure Department Selection** page allows you to specify how you assign department groups to users in Content Server: using a menu or a Department dialog.

To open the **Configure Department Selection** page from the Content Server Administration page, click **Configure Department Selection** in the **Users and Groups Administration** section.

For more information on the **Configure Department Selection** page, see *OpenText Content Server - Administering Groups and Domains (LLESWBU-AGD)*.

The Data Policies Usage Privilege

The **Data Policies** Business Administration usage privilege enables access to the following administration pages:

Administer Item Control

The **Administer Item Control** page allows you to configure version control settings and to enable the **Group Reserve Capability**.

To open the **Administer Item Control** page from the Content Server Administration page, click **Administer Item Control** in the **System Administration** section.

For more information on the **Administer Item Control** page, see "Administering Item Control" on page 335.

Administer MIME Types and Categories

The **Administer MIME Types and Categories** page allows you to associate any available MIME type with an existing Category.

To open the **Administer MIME Types and Categories** page from the Content Server Administration page, click **Administer MIME Types and Categories** in the **System Administration** section.

For more information on the **Administer MIME Types and Categories** page, see “Associating MIME Types and Categories” on page 237.

Administer Modified Date Triggers

The **Administer Modified Date Triggers** page allows you to control whether or not changes to an item’s permissions or to the Categories and attributes that are applied to it affect the **Modified** date of the item.

To open the **Administer Modified Date Triggers** page from the Content Server Administration page, click **Administer Modified Date Triggers** in the **System Administration** section.

For more information on the **Administer Modified Date Triggers** page, see “Administering Modified Date Triggers“ on page 341.

Configure Access Control

The **Configure Access Control** page allows you to control the level of discretion that is available to users and administrators who control access to Content Server items.

To open the **Configure Access Control** page from the Content Server Administration page, click **Configure Access Control** in the **System Administration** section.

For more information on the **Configure Access Control** page, see “Configuring Access Control“ on page 371.

Configure Attribute Value Requirements

The **Configure Attribute Value Requirements** page allows you to specify that users do not have to define attribute values for certain object types, even for required attributes defined on the **Administer Additional Node Attributes** page.

To open the **Configure Attribute Value Requirements** page from the Content Server Administration page, click **Configure Attribute Value Requirements** in the **System Administration** section.

For more information on the **Configure Attribute Value Requirements** page, see *OpenText Content Server - Category and Attribute Administration (LLESWAT-AGD)*.

Collections General Settings

The **Collections General Settings** page allows you to configure various Collections settings.

To open the **Collections General Settings** page from the Content Server Administration page, click **Collections General Settings** in the **Collections Administration** section.

For more information on the **Collections General Settings** page, see *OpenText Content Server - Administering Collections (LLESCL-AGD)*.

Configure History General Settings

The **Configure History General Settings** page allows you to set the number of recently accessed items to track for each user and the number of days to keep this information.

To open the **Configure History General Settings** page from the Content Server Administration page, click **Configure History General Settings** in the **Recommender Administration** section.

For more information on the **Configure History General Settings** page, see *OpenText Content Server Admin Online Help Collection - Recommender Administration (LLESREC-AGD)*.

Configure Mandatory Search Terms

The **Configure Mandatory Search Terms** page allows you to define search term restrictions for users based on the Content Server user group that they belong to.

To open the **Configure Mandatory Search Terms** page from the Content Server Administration page, click **Configure Mandatory Search Terms** in the **Search Administration** section.

For more information on the **Configure Mandatory Search Terms** page, see *OpenText Content Server - Administering Search (LLESWBS-AGD)*.

Configure Allowable Prospectors Queries

The **Configure Allowable Prospectors Queries** page allows you to configure the types of queries that can be used with Prospectors.

To open the **Configure Allowable Prospectors Queries** page from the Content Server Administration page, click **Configure Allowable Prospectors Queries** in the **Prospectors** section.

For more information on the **Configure Allowable Prospectors Queries** page, see *OpenText Content Server Admin Online Help Collection - Prospectors Administration (LLESPRO-AGD)*.

The Facets and Columns Usage Privilege

The **Facets and Columns** Business Administration usage privilege enables access to the following administration pages:

Configure Document Classes

The **Configure Document Classes** page allows you to add Content Server Document Classes and their underlying MIMEType Aliases and to modify existing ones.

To open the **Configure Document Classes** page from the Content Server Administration page, click **Configure Facets** in the **Server Configuration** section, and then click **Configure Document Classes**.

For more information on the **Configure Document Classes** page, see “Configuring Faceted Browsing” on page 49.

View Facets Volume

The **View Facets Volume** link opens the Facets Volume, if you have permission to access it. (The Facets and Columns usage privilege does not give you permission to access the Facets Volume. Permission to access the Facets Volume must be assigned to you explicitly.)

To open the **View Facets Volume** page from the Content Server Administration page, click **Configure Facets** in the **Server Configuration** section, and then click **View Facets Volume**.

For more information on the **View Facets Volume** page, see "Working with the Facets Volume" on page 52.

The Query Audit Log Usage Privilege

The **Query Audit Log** Business Administration usage privilege enables access to the following administration page:

Query Audit Log

The **Query Audit Log** page allows you to track events that occur in Content Server.

To open the **Query Audit Log** page from the Content Server Administration page, click **Query Audit Log** in the **System Administration** section.

For more information on the **Query Audit Log** page, see "Administering Event Auditing" on page 319.

The Recycle Bin Configuration Usage Privilege

The **Recycle Bin** Business Administration usage privilege enables access to the following administration page:

Recycle Bin Settings

The **Recycle Bin Settings** page allows you to configure the appearance and behavior of the Recycle Bin.

To open the **Recycle Bin Settings** page from the Content Server Administration page, click **Recycle Bin** in the **System Administration** section.

For more information on the **Recycle Bin Settings** page, see "Recycle Bin Administration" on page 405.

The Reminder Administration Usage Privilege

The **Reminder Administration** Business Administration usage privilege enables access to the following administration pages:

Edit Reminder mail and notification formats

The **Edit Reminder mail and notification formats** page allows you to set default Reminder messages.

To open the **Edit Reminder mail and notification formats** page from the Content Server Administration page, click **Configure Email-Notification Format** in the **Reminder Administration** section.

For more information on the **Edit Reminder mail and notification formats** page, see *OpenText Content Server - ReminderAdministration (LLESRSB-AGD)*.

Reminder settings

The **Reminder settings** page allows you to configure default settings for all Reminders.

To open the **Reminder settings** page from the Content Server Administration page, click **Settings and defaults** in the **Reminder Administration** section.

For more information on the **Reminder settings** page, see *OpenText Content Server - ReminderAdministration (LLESRSB-AGD)*.

The User and Group Configuration Usage Privilege

The **User and Group Configuration** Business Administration usage privilege enables access to the following administration pages:

Configure User Name Display

The **Configure User Name Display** page allows you to specify the format used to display Content Server user names.

To open the **Configure User Name Display** page from the Content Server Administration page, click **Configure User Name Display** in the **Users and Groups Administration** section.

For more information on the **Configure User Name Display** page, see "Configuring User Settings" on page 427.

User Tab Permissions

The **User Tab Permissions** page allows you to assign users and groups varying levels of access to Content Server user pages. For example, you can allow users to modify their own user page, anyone's user page, or no user pages at all.

To open the **User Tab Permissions** page from the Content Server Administration page, click **User Tab Permissions** in the **Users and Groups Administration** section.

For more information on the **User Tab Permissions** page, see "Setting User Tab Permissions" on page 11.

21.2.3 Collections Command and Collections Operation Usage Privileges

Collections usage privileges fall under the **Collections Command** or **Collections Operation** usage types. For more information, see *OpenText Content Server - Administering Collections (LLESCL-AGD)*.

Tip: There is also a **Collect** usage privilege that is of the **Multi-Select Command** usage type. See “Other Usage Privileges” on page 368

Table 21-3:

Usage Type	Usage Name	Default Setting	Reason to Restrict	Effect
Collections Command	Queue for Indexing	Restricted	performance, user experience	Allows you to see and use a **Queue for Indexing** command that appears in the Collection’s **More Actions** menu to submit Content Server Collection items in bulk for addition to the Search Index.
Collections Command	Queue Thumbnail Generation	Restricted	performance, user experience	Allows you to request thumbnails to be generated.
Collections Command	Copy Items	Unrestricted	user experience	Allows you to see and use a multi-select **Copy** button to bulk copy multiple Content Server items. (Actual copy of one or more items. Not a copy of one or more Collection items to another Collection.)

Usage Type	Usage Name	Default Setting	Reason to Restrict	Effect
Collections Command	Move Items	Unrestricted	user experience	Allows you to see and use a multi-select **Move** button to bulk move multiple Content Server items. (Actual move of one or more items. Not a move of one or more Collection items to another Collection.)
Collections Command	Delete Items	Restricted	performance, security	Allows you to see and use a multi-select **Delete** button to bulk delete multiple Content Server items. (The button deletes the actual Content Server items. It does not simply remove items from the Collection.)
Collections Command	Copy Items to Another Collection	Unrestricted	user experience	Allows you to see and use a **Copy Items to Another Collection** command that appears in the Collection’s **More Actions** menu to copy Collection items in bulk to another Collection.

Usage Type	Usage Name	Default Setting	Reason to Restrict	Effect
Collections Command	Make Disk Image	Restricted	performance, security	Allows you to see and use a **Make Disk Image** command that appears in the Collection's **More Actions** menu to bulk copy Collection items to a Disk Image (`ISO` file).
Collections Command	Move Items to Another Collection	Unrestricted	user experience	Allows you to see and use a **Move Items to Another Collection** command that appears in the Collection's **More Actions** menu to move Collection items in bulk to another Collection.
Collections Command	Remove Items from Collection	Unrestricted	user experience	Allows you to see and use a **Remove Items from Collection** command that appears in the Collection's **More Actions** menu to remove Collection items in bulk from the Collection.
Collections Command	Download as Spreadsheet	Restricted	performance, security	Allows a user to bulk export Content Server item metadata to a spreadsheet (`.csv` file).

Usage Type	Usage Name	Default Setting	Reason to Restrict	Effect
Collections Command	Zip & Download Command	Unrestricted	performance	Allows you to see and use a **Zip & Download** command that appears in the Collection’s **More Actions** menu to bulk copy Content Server items from the Collection in a compressed archive.
Collections Command	Zip & Email Command	Unrestricted	performance	Allows you to see and use a **Zip & E-mail** command that appears in the Collection’s **More Actions** menu to email a compressed archive containing Content Server items copied from the Collection.
Collections Command	Print Command	Unrestricted	performance	Allows you to see and use a **Print** command that appears in the Collection’s **More Actions** menu to print multiple Content Server items from the Collection.

Usage Type	Usage Name	Default Setting	Reason to Restrict	Effect
Collections Command	Apply Categories	Unrestricted	performance	Allows you to see and use an **Apply Categories** command that appears in the Collection's **More Actions** menu to apply Categories and attributes to multiple Content Server items. (Categories are applied to actual Content Server items, not merely to the Collection items.)
Collections Command	Create Searchable Collection	Unrestricted	performance	Allows you to enable searches when creating a new Collection.
Collections Operation	Collect All Search Results	Restricted	performance	Allows you to add all the items returned by a search query into a Collection.
Collections Operation	Custody Details in Disk Image	Restricted	performance	Allows you to provide information about the Content Server software environment, when the Collection was created, completeness details, etc.

21.2.4 Form Submittable Storage and Form Revisable Storage Usage Privileges

Forms usage privileges fall under the **Form Submittable Storage** and **Form Revisable Storage** usage types. For more information see:

- *OpenText Content Server - Forms Administration (LLESFRM-AGD)*
- *OpenText Content Server - Forms Administration (LLESFRM-AGD)*
- *OpenText Content Server - WebReports (LLESWEBR-UGD)*

Table 21-4: Content Server Usage Privileges

Usage Type	Usage Name	Default Setting	Reason to Restrict	Effect
Form Revisable Storage	SQL Table	Unrestricted	user experience	Allows users to select the SQL Table revision mechanism when they create a Form and select a template for which a database table exists.
Form Submittable Storage	SQL Table	Unrestricted	user experience	Allows users to select the SQL Table submission mechanism when they create a Form and select a template for which a database table exists.
Form Submittable Storage	User Revisable Records (SQL)	Unrestricted	user experience	Allows users to select the User Revisable Records (SQL) mechanism when they create a Form and select a template for which a database table exists.

Usage Type	Usage Name	Default Setting	Reason to Restrict	Effect
Form Submittable Storage	Initiate WebReport (SQL)	Unrestricted	user experience	**Initiate WebReport** that is similar to **SQL Table**. The main difference is that when the data is stored in the SQL table, the primary key, or SEQ, is identified and passed to a WebReport which is initiated immediately after the form submission.

21.2.5 Item Handler Task Operation Usage Privileges

The Item Handler is a powerful workflow feature. It usage privileges are restricted by default. For more information, see *OpenText Content Server - Workflow Administration (LLESWFW-AGD)*.

Tip: Note that there is also an **Item Handler** usage privilege under the **Workflow Task Type** usage type. See “Workflow Usage Types” on page 367.

Table 21-5: Content Server Usage Privileges

Usage Type	Usage Name	Default Setting	Reason to Restrict	Effect
Item Handler Task Operation	Versioning	Restricted	security	Allows you to add versions to any items in the system as any system user regardless of your permissions to the item.
Item Handler Task Operation	Move/Copy	Restricted	security	Allows you to make copies of any item in the system and perform the copy as any system user.

Usage Type	Usage Name	Default Setting	Reason to Restrict	Effect
Item Handler Task Operation	Categories	Restricted	security	Allows you to change metadata for any item in the system and perform the change as any system user.
Item Handler Task Operation	Folder Definitions	Restricted	security	Allows you to create folders anywhere in the system and perform the creation as any system user.

21.2.6 Renditions Usage Privileges

Renditions usage privileges regulate the ability of users to create renditions of documents. For more information, see *OpenText Content Server - Renditions (LLESRND-UGD)*.

Table 21-6: Content Server Usage Privileges

Usage Type	Usage Name	Default Setting	Reason to Restrict	Effect
Renditions	Make Rendition	Restricted	user experience	Allows users to create an Ad Hoc Rendition of a Document.
Renditions	Subscribe to Rendition	Restricted	user experience	Allows users to subscribe individual Documents for renditioning whenever new Versions are added.

21.2.7 Search Usage Privileges

Usage privileges in the **Search** usage type regulate the way that Content Server returns results to users. For more information, see *OpenText Content Server - Administering Search (LLESWBS-AGD)*.

Table 21-7: Content Server Usage Privileges

Usage Type	Usage Name	Default Setting	Reason to Restrict	Effect
Search	See Unpermissioned Result Counts	Restricted	security	Allows you to see the true search result count from the Search Engine that is shown to users with the System Administration Rights privilege, rather than the estimate that is shown to non-administrative users.
Search	Results with See Permission	Restricted	security	Allows users to know if documents related to a topic exist, even if they cannot access the documents, and then ask permission for access. This enables users to view search results if they have at least *See* permission, instead of the standard *See Contents* permission.

21.2.8 WebReports Usage Privileges

WebReports usage privileges regulate your ability to perform certain WebReports operations. For more information, see:

- *OpenText Content Server - WebReports (LLESWEBR-UGD)*
- *OpenText Content Server - WebReports (LLESWEBR-UGD)*

Table 21-8: Content Server Usage Privileges

Usage Type	Usage Name	Default Setting	Reason to Restrict	Effect
WebReports	Run As	Unrestricted	security, user experience	Allows you to run a WebReport as a different user without having the System Administration Rights privilege, and possibly to view items and content that you do not have permission to access. (WebReports Audit shows the actual user that triggered the report.)
WebReports	WR Trigger Tab	Unrestricted	user experience	Allows you to access the **WebReports Trigger** tab of a Content Server item without having the System Administration Rights privilege.

21.2.9 Workflow Usage Types

Workflow usage types include the **Workflow Task Type**, **Workflow Features** and **Workflow Data Type** usage types. Workflow usage types enable heightened privileges for workflow designers. For more information, see *OpenText Content Server - Workflow Administration (LLESWFW-AGD)* and *OpenText Content Server - Workflow Maps (LLESWFP-UGD)*.

Table 21-9: Content Server Usage Privileges

Usage Type	Usage Name	Default Setting	Reason to Restrict	Effect
Workflow Data Type	Initiate Workflow From Item Replacement Tags	Unrestricted	user experience	Allows a workflow designer to use dynamic replacement tags that refer to a Content Server item. The tags are replaced by item values when a user clicks **Initiate <*item*> Workflow** on an item’s **Functions** menu.
Workflow Task Type	Item Handler	Restricted	security	Allows you to interact with documents as a user of your choosing. Full access to the Item Handler allows you to update items and item metadata as any user in the system. The audit log shows the configured user, not the workflow, as the user that made the changes.

Usage Type	Usage Name	Default Setting	Reason to Restrict	Effect
Workflow Features	Agent Performers	Restricted	performance	Allows you to be assigned workflow tasks that are performed by the workflow agent.
Workflow Features	Assign to Workflow Agent	Restricted	security	Allows you to assign workflow tasks to the workflow agent. This privilege could be used to do malicious actions in bulk.

21.2.10 Other Usage Privileges

The usage privileges that are documented in this section are ones that are the only usage privilege in their usage type. For example, the **View Storage Rules** usage privilege is the only privilege that has a **Storage Provider** usage type, so it is documented in this section.

Table 21-10: Content Server Usage Privileges

Usage Type	Usage Name	Default Usage Status	Reason to Restrict	Effect	More Information
Content Sharing Operation	Share Item with OpenText Core	Restricted	user experience	Allows users to share items in OpenText™ Core using Content Sharing.	*OpenText Content Server - Content Sharing (LLESEFS-AGD)*
Best Bets Administration	Set Best Bets Value	Restricted	user experience	Allows users to apply or edit Best Bets values.	*OpenText Content Server - Administering Search (LLESWBS-AGD)*

Usage Type	Usage Name	Default Usage Status	Reason to Restrict	Effect	More Information
Storage Provider	View Storage Rules	Restricted	security	Allows you to see and use a **Storage Rules** option in the **Tools** global menu to view (but not edit) Content Server Storage Rules.	“Configuring Storage Rules” on page 386
Web Forms Features	Execute SQL Lookup	Unrestricted	user experience	Allows users the ability to execute database lookups.	*OpenText Content Server - Web Forms Administration (LLESWFM-AGD)*
Web Administration	Web Admin	Restricted	security, user experience	Allows you to access the Content Server Administration page.	“Configuring Basic Server Parameters” on page 73
Recycle Bin Administration	Recycle Bin Manager	Restricted	security, user experience	Allows you to view, restore, and purge any items in the Recycle Bin. Allows you to access the Recycle Bin even if user access to the Recycle Bin has been disabled.	“Recycle Bin Administration“ on page 405

Usage Type	Usage Name	Default Usage Status	Reason to Restrict	Effect	More Information
Multi-Select Command	Collect	Unrestricted	user experience	Allows you to see and use a multi-select **Collect** button to bulk add multiple Content Server items to a Collection.	*OpenText Content Server - Administering Collections (LLESCL-AGD)*
Warehouse Administrati on	Warehouse Manager	Restricted	security	Allows you to see and change an item's metadata, including the owner of an item.	*OpenText Content Server - Administering Transport (LLESTRP-AGD)*
Facet Administrati on	Knowledge Manager	Restricted	performance, user experience	Allows you to access the Facets Volume from the **Enterprise** global menu and to create Content Server facets and columns.	"Configuring Faceted Browsing" on page 49

Chapter 22

Configuring Access Control

Settings on the **Configure Access Control** page affect how item permissions work in Content Server. For example, you can disable Owner, Owner group, and Public Access permissions so that permission to items is governed exclusively by explicit Access Control Entries (ACEs).

In the **Permissions Page Access** section, you can set the minimum permission that is required for a Content Server user to view an item's **Permissions page.**

- If you select **See Contents**, users that have **See Contents** permission (or higher) to an item see a **Permissions** option in the item's **Functions** menu, and can view the item's **Permissions** page. They cannot make changes to the item's permissions, however, unless they have **Edit Permissions** access to the item.
- If you select **Edit Permissions** (the default option), users do not see a **Permissions** option in the item's **Functions** menu unless they have **Edit Permissions** access to the item. Users with **Edit Permissions** access can view an item's **Permissions** page and make changes to the item's permissions.

In the **Default Access** section, you can restrict the ability of Content Server users that do not have the **System Administration rights** privilege to change an item's permissions. By default, none of the following options are enabled.

- If you select **Restrict "Grant Access" to Groups only**, ACE assignments can be granted only to groups. If this option is cleared, access to an item can be granted to individual users.
- If you select **Restrict restoring "Owner Access" to System Administrators**, only Content Server administrators can restore the Owner of an item. If this option is not selected, any user with **Edit Permissions** access to an item can restore its Owner.
- If you select **Restrict restoring "Owner Group Access" to System Administrators**, only Content Server administrators can restore an item's Owner Group. If this option is not selected, any user with **Edit Permissions** access can restore an item's Owner Group.
- If you select **Restrict restoring "Public Access" to System Administrators**, only Content Server administrators can restore **Public Access** to an item. If this option is not selected, any user with **Edit Permissions** access can restore **Public Access** to an item.

In the **Moving Items across Workspaces** section, you can select **Always inherit the permissions from target destination**, which forces an item's permissions settings to be inherited from the destination when it is moved from one workspace to a different workspace. (This setting has no effect on items that are moved within the same workspace.) For more information about how copying or moving an item affects its permissions, see *OpenText Content Server - Get Started (LLESRT-UGD)*.

In the **eDiscovery Mode Access** section, you can select **Enable eDiscovery mode access**, which allows users to be assigned the **eDiscovery Rights** system privilege. Users with this system privilege can select **Enable eDiscovery Mode** on their **My General Settings** page. (For more information, see *OpenText Content Server - Users and Groups (LLESWBU-UGD)*.) If **Enable eDiscovery mode access** is cleared, no user can be assigned the **eDiscovery Rights** system privilege, and the option to assign this system privilege does not appear on the **Add New User** or the **General Info for: <*user*>** page.

22.1 To Configure Access Control

To configure access control:

1. In the **System Administration** section of the Content Server Administration page, click **Configure Access Control**.
2. Optional In the **Permissions Page Access** section, select **Edit Permissions** to restrict access to an item’s **Permissions** page to users with **Edit Permissions** access to the item.
3. Optional In the **Default Access** section:

   - Select **Restrict "Grant Access" to Groups only** to allow access to items to be granted only to groups, not individual users.
   - Select **Restrict restoring "Owner Access" to System Administrators** to allow Owner Access to be restored only by a Content Server administrator.
   - Select **Restrict restoring "Owner Group Access" to System Administrators** to allow Owner Group Access to be restored only by a Content Server administrator.
   - Select **Restrict restoring "Public Access" to System Administrators** to allow Public Access to be restored only by a Content Server administrator.

4. Optional In the **Moving Items across Workspaces** section, select **Always inherit the permissions from target destination** to ensure that an item that is moved from one workspace to another inherits its permissions from the target workspace.
5. Optional In the **eDiscovery Mode Access** section, select **eDiscovery Mode access** to allow users to be assigned the **eDiscovery Rights** system privilege.
6. Click **Update** to save your changes.

Chapter 23

Working with Copy and Delete Item Operations

The copy and delete item function enables users to copy and delete multiple items at one time. You can change the default settings for the entire system.

23.1 Configuring the Status Page for Multi-Select Actions

You can allow users to see a status page that shows the progress of items that are in the process of being copied, moved, or deleted.

When you set the display progress to `yes`, you can specify the number of items that get processed before the page refreshes itself. When the display progress is set to `no`, the status page does not display until all items have been moved, copied, or deleted.

23.1.1 To Configure the Status Page for Multi-Select Actions

To configure the status page for multi-select actions:

1. In the **System Administration** section on the Administration page, click the **Configure Status Page for Multi-Select Actions** link.
2. Do one of the following:
   - Click the **Yes, and update progress display after `X` items processed** radio button, and then type a number in the text field to specify the number of items you want to process before the page refreshes.
   - Click the **No, just show the results when finished** radio button.
3. Click the **OK** button.

23.2 Configuring the Operations for Copy, Delete and Move

You can specify how Content Server commits batch copy or delete operations to the database—either individually or as a group. For a request that contains multiple items, Content Server defaults to processing all of the copy, delete, or move operations in a single transaction. If a single item in the transaction fails, the entire batch rolls back to its original state and nothing is committed to the database. Alternatively, you can configure Content Server to commit copy, delete, or move operations to the database item by item. With this setting enabled, if an item fails, it does not cause the entire operation to fail. Any item that is processed successfully is committed to the database.

You can also configure the move throttle control setting, which limits the number of items that users can move from one Content Server location to another.

Note: The move control throttle setting may prevent users from moving items even when they have apparently selected fewer items than the maximum allowed by the move throttle. This is because items counted towards the move throttle control setting include containers, such as Folders, and items within containers.

For example, if the `Maximum approximate number of objects allowable in one move` is set to 1,000, and a user selects 100 Documents and a Folder containing 900 Documents, the move throttle control will prevent the move operation.

23.2.1 To Modify the Copy, Delete, and Move Operation Settings

To modify the Copy, Delete, and Move Operation settings:

1. In the **System Administration** section of the Content Server Administration page, click **Configure the Operations for Copy, Delete and Move**.
2. On the **Configure the Operations for Copy, Delete and Move** page, enable one of the following settings in the **Copy** and **Delete** sections:

   - **Commit the transactions after all items were processed successfully**, which commits the database transaction when all items have been processed.

     Note: If one item in the transaction fails, the entire transaction fails and nothing is committed to the database.

   - **Commit the transaction for each item processed successfully**, which commits the database transaction for each processed node.

     Note: For the Copy function, this operation copies one node at a time and commits the database transaction using a top-down scheme. However, for the Delete function, the operation deletes one node at a time and commits the database transaction using a bottom-up scheme.

3. Optional In the **Move** section, select the **Enable the move throttle control** check box, and then type the maximum number of objects allowed in a move in the **Maximum approximate number of objects allowable in one move** box.
4. Click **Update**.

Chapter 24

Database Connection Administration

The **Database Connection Administration** section of the Content Server administration pages allows you to:

- Set or alter the encryption key used to protect your connection information. For more information, see "To Create a Connection Encryption Key" on page 377.
- List database information for external databases. For more information, see *OpenText Content Server - Web Forms Administration (LLESWFM-AGD)*.
- Create, view, and edit database connections. For more information, see "Managing Secure Database Connections" on page 375.
- Create, view, and edit executable database lookups. For more information, see "Managing Secure Database Lookups" on page 378.

24.1 Managing Secure Database Connections

Content Server database lookups are executed using JavaScript in the HTML template view. They consist of a secure database connection and a secure database lookup. Before you can create a secure database lookup, you must first create a secure database connection to the database that contains the information to be looked up.

Manage Secure Database Connections

The **Manage Secure Database Connections** link in the **Database Connections Administration** section allows you to view, modify, and create database connections. A database connection allows you to connect to Content Server or an external SQL database for use by LiveReports, or by a secure database lookup in an HTML view of a Form Template. You cannot delete a database connection if it is in use.

By default, only the administrator can create secure database connections and secure database lookups. Any user can execute lookups. Content Server users who try to perform a database lookup request without permission to use the database lookup function receive an error.

When you create a connection encryption key, all new and existing database connection passwords are encrypted. When you update the encryption key, all of the connection objects that use the key are updated. OpenText recommends that you create a connection encryption key, otherwise, the passwords for your database connections are stored in plain text in the database.

Note: If you want to grant permission to users who want to be able to create database connections and lookups, or if you want to restrict which users can execute database lookups, you must modify the user restrictions for these functions on the **Administer Usage Privileges** page in the **System Administration** section. For more information about configuring restrictions for either executing the database lookup function or creating connections or lookups, see "Administering Object Privileges and Usage Privileges" on page 343.

24.1.1 To Create or Modify a Secure Database Connection

To create or modify a secure database connection:

1. In the **Database Connections Administration** area, click the **Manage Secure Database Connections** link.

2. On the **Database Connections** page:

   - If you want to view or modify an existing secure database connection, from the list of existing connections, click the name link of the database connection you want to view or modify.
   - If you want to create a new secure database connection, from the **Add Item** menu select **Database Connection**.

3. On the **Add: Database Connection** page, or the **Edit: <*name*> Database Connection** page, from the **RDBMS Server Type** list, select the type of relational database to which you wish to connect.

   Note: Based on the database system you select, different fields display below.

   Microsoft SQL Server will only be available as a choice on the **RDBMS Server Type** list if Content Server is running on a Microsoft Windows server.

   - For Microsoft SQL Server, you must specify the **User Name** and **Password** of a Microsoft SQL Server user account with permission to access the database, along with the **SQL Server Name** and **SQL Database Name** to which the connection is made.

   - For Oracle Server, you must specify the **User Name** and **Password** used to connect to the Oracle server, and the **Service Name**, which is the connect string for the database service to which the connection is made.

   - For HANA Server, you must specify the **User Name** and **Password** used to connect to the HANA server, the **HANA Server**, which is the connect string for the database service to which the connection is made, along with the **HANA Schema**.

   - For PostgreSQL Server, you must specify the **User Name** and **Password** of a PostgreSQL Server user account with permission to access the database, along with the **PostgreSQL Server Name** and **PostgreSQL Database** to which the connection is made.

4. The **Dependent Lookups** box displays regardless of the database system you select. You cannot modify this field while creating a database connection.

5. Specify **Name**, **Description**, **Categories**, and **Create In** parameters as you would when adding any item to Content Server.

   Note: The **Name** you specify for the database connection must be unique among all database connections.

6. Click **Add**.

24.1.2 To Modify Database Connection Properties

To modify database connection properties:

1. On the Content Server administration page, in the **Database Connections Administration** area, click the **Manage Secure Database Connections** link.

2. On the **Database Connections** page, click the database name link to view and modify the database connection's properties.

3. Click **Add Version**.

   1. Once a database connection is created, you cannot change the **RDBMS Server Type**.
   2. The **Dependent Lookups** box displays regardless of the database system you select. You can view names of all current Database Lookups that require the current database connection. You cannot modify any Database Lookups on this page. If you want to modify a Database Lookup see "To Modify Database Lookup Properties" on page 379.

24.1.3 To Create a Connection Encryption Key

To create a connection encryption key:

1. On the Content Server administration page, in the **Database Connections Administration** area, click the **Connection Encryption Key** link.

2. In the **Connection Encryption Key** box, enter a key. The key can contain any combination of letters, numbers, or special characters. There is no limit on the length of the key.

3. Click **Submit**.

24.2 Managing Secure Database Lookups

A secure database lookup allows the administrator to create an SQL statement that can be executed in response to a user action on a WebForm HTML view.

The following describes the fields, required and optional, when creating a database lookup:

- A lookup requires a secure database connection, which defines the specific database on which the SQL database statement will be executed. The **Database Connection** field requires that you identify the secure database connection for this lookup. The secure database connection must be created first, and you can find information about creating a secure database connection in "Managing Secure Database Connections" on page 375. Once your secure database connection has been created, you need to select it in this box.
- The **SQL statement to execute** field defines the SQL statement that will be executed against the specified database connection and may optionally accept parameters passed from a WebForm. To bind the values passed in from the form to the SQL statement, the administrator will use standard SQL bind syntax, adding `:A <n>` to the SQL statement to represent the <*n*>th parameter. For example, `:A1` is replaced by the value of the first parameter, and `:A2` is replaced by the value of the second parameter, and so on.
- If the **Filter Output Based On Permissions** box is selected, then the **SQL statement to execute** must include the **DataID**, **OwnerID**, and **PermID** columns from the `DTree` table in a Content Server database. With those three columns, the lookup will execute, and only rows that the current user has **See** permission to access will be returned in the output data. Rows that the current user does not have **See** permission to access will be removed from the output data.
- **Name**, **Description**, **Categories**, and **Create In** are standard fields that can be used whenever anyone creates any type of node in Content Server.

  The **Name** and **Create In** fields are required. The **Name** you enter must be unique, and the Name value must be specified in the WebForm HTML view JavaScript to specify which lookup will be executed.

24.2.1 To Create a Database Lookup

To create a database lookup:

1. On the Content Server administration page, in the **Database Connections Administration** area, click the **Manage Secure Database Lookups** link.
2. On the **Database Lookups** page, from the **Add Item** menu, select **Database Lookup**.
3. On the **Add: Database Lookup** page, specify the following information:
   - **Database Connection**, which is the name of the connection object representing the database system to which you want to connect.

- **SQL statement to execute**, which is the SQL statement that is executed against the specified database connection.
- **Filter Output Based On Permissions**, which is whether the results of the lookup should be limited by the permissions of the user. If selected, you must have specified DataID, OwnerID, and PermID columns from the DTree table in the **SQL statement to execute** field above.

4. Specify **Name**, **Description**, **Categories**, and **Create In** parameters as you would when adding any item to Content Server.
5. Click **Add**.

24.2.2 To Modify Database Lookup Properties

To modify database lookup properties:

1. On the Content Server administration page, in the **Database Connections Administration** area, click the **Manage Secure Database Lookups** link.
2. On the **Database Lookups** page, click the lookup name link to view and modify the properties of the database lookup.
3. Click **Add Version**.

Part 5

Item Administration

Chapter 25

Storage Providers and Storage Management

Content Server allows you to store Documents and other items in multiple locations. You can configure Content Server to use several different Storage Providers, which allows Content Server items to be stored wherever is most appropriate, according to the Storage Provider Rules that you implement. Storage Providers and Storage Provider Rules can be added, deleted, or modified by the Content Server administrator.

25.1 Managing Internal and External Storage

Content Server can store items internally in the database or externally on the file system.

When you use internal storage, both the content and *metadata* (data describing a Content Server item) are stored in the database. When you use external storage, only an item’s metadata is stored in the database; the content of the files is stored on the file system.

When an item is added to Content Server, the system creates a record for it in the `ProviderData` table and in other Content Server database tables. The `ProviderData` table stores information that tells Content Server where to retrieve the file when users request to view or fetch it. In the case of internal storage, the `ProviderData` table stores the internal database location of the file. In the case of external storage, the `ProviderData` table stores the physical path of the file on the file system.

Note: When you use external document storage, Content Server uses a numbering algorithm to name files so it can keep track of multiple versions of the same file. Content Server does not store files on the file system under the same names as they had when they were copied from users' disks. For example, if a user adds a file called `Expense12Mar.xls` to Content Server, its name in the external storage directory may be something like `2934eriw.233`.

25.1.1 Setting Up an External File Store

If you locate an External File Store (EFS) on the primary Content Server host, writing and retrieving documents may be slightly faster, because there is no network delay, however testing by OpenText has shown that this performance improvement may be marginal compared to locating the EFS on a remote host. The improvement may be more significant if you are operating in an environment where the network is very busy. If this is the case, consider placing the components of the Content Server system on their own isolated subnetwork.

When you add External Document Storage, you give the new Storage Provider a name and specify its location. Before you do:

- Create the folder that you want to use as the root of the External File Store. Content Server will not create the folder if it does not exist.
- If the EFS is not on the same host as your primary Content Server installation, map or mount the folder on the primary Content Server host. For Linux, use an NFS mount. For Windows, use a UNC path. (Do not map a drive letter.)
- Make sure that the remote file store folder is owned by the Content Server user. Create a user with the same name, password, and privileges on both the primary Content Server host and the External File Store host. The servers on the primary Content Server host must run as this user and the remote EFS folder must be owned by this user. For more information about the permissions that a Content Server user must have, see *OpenText Content Server - Installation Guide (LLESCOR-IGD)*.

  Try connecting to the folder from the primary Content Server host as the Content Server user to test whether you can access it and write to it. If you encounter permission or ownership problems when performing this test, correct the problems before you create the Content Server database.

25.2 Configuring Storage Providers

Storage Providers enable you to store Content Server Documents and other items. Storage providers include:

- External folders
- Databases
- OpenText™ Archive Center

Storage Provider Rules determine which Storage Provider stores a given item based on rule settings and the characteristics of the item.

Content Server always creates an internal database storage provider and a ZeroByte storage provider. The default Content Server storage rules send zero-byte files to the ZeroByte storage provider and objects without content to the internal database storage provider. Each Content Server instance has a default Storage Provider that cannot be modified or deleted. If you configure an external storage provider during the initial setup of Content Server, it becomes the default storage for documents, emails, and all other items. Otherwise, the internal database storage provider becomes your default storage provider.

For more information about Storage Provider Rules, see “Configuring Storage Rules” on page 386.

Administrators can audit the movement of content from one Storage Provider to another. By default, the `Provider Changed` audit interest is turned off. The audit details for this event include the original Storage Provider name, the new Storage Provider name, and the name of the user who moved the content. Every Document in Content Server displays the name of its Storage Provider on the **Versions** tab of the Document's Properties page. Users with the proper permissions can view the entire list of Storage Provider Rules. This list includes the Storage Provider rule, and the name and type of the Storage Provider.

25.2.1 To Add a Storage Provider

To add a Storage Provider:

1. On the Content Server Administration page, in the **Storage Provider Settings** area, click **Configure Storage Providers**.

2. On the **Configure Storage Providers** page, from the **Add Item** list, click the type of Storage Provider you want to add.

3. On the **Add New Logical Storage Provider** page, in the **Name** field, type a name for the Storage Provider.

4. In the **Configuration** field, type the absolute path to the Storage Provider.

   Note: The *absolute path* applies to external storage directories. If the Storage Provider type is something other than an external directory, you may need to specify a different configuration path in the **Configuration** field. After you add a Storage Provider, you must define rules for it.

5. Click **Submit**.

6. Restart Content Server.

25.2.2 To Modify a Storage Provider

To modify a Storage Provider:

1. On the Content Server Administration page, in the **Storage Provider Settings** area, click **Configure Storage Providers**.

2. On the **Configure Storage Providers** page, click **Edit** next to the storage provider you want to edit.

3. In the **Configuration** field, type an absolute path to the new Storage Provider.

   Note: The *absolute path* applies to external storage directories. If the storage provider type is something other than an external directory, you may need to specify a different configuration path in the **Configuration** field.

   If you change the storage provider's configuration path, you must manually move existing content from the old location to the new location.

4. Click **Submit**.

5. Restart Content Server.

25.2.3 To Delete a Storage Provider

Note: You cannot delete a Storage Provider when it is in use.

To delete a Storage Provider:

1. On the Content Server Administration page, in the **Storage Provider Settings** area, click **Configure Storage Providers**.
2. On the **Configure Storage Providers** page, in the **Actions** column for the Storage Provider you want to delete, click **Delete**.
3. Click **OK** in the confirmation dialog.
4. Restart Content Server.

25.3 Configuring Storage Rules

You can set individual binary rules and create an ordered association between the rules and Storage Providers to determine where Documents are stored.

Tip: You do not need to restart Content Server after you modify Storage Providers, rules, and their associations.

You can configure as many storage rules as you want, however, OpenText recommends that you keep the number of storage rules below 12. Storage rules are evaluated whenever a Document is added to Content Server or whenever a Content Move job is started. When a Document is added, the rules are evaluated in order from the top of the list to the bottom. If the Document does not meet any of the defined rules, it is stored in the *default Storage Provider*, which always appears last on the list and cannot be configured or deleted.

A storage rule consists of a rule name, one or more conditions, and a storage target which is selected if all the conditions are true. After a rule is created, you can modify it, delete it, and change its order in the list. When you add a new rule, it will appear above the current rule by default.

For each rule type you add, you specify the value of the rule, represented below by the **?** in the **Value** field.

The following rules are available by default when Content Server is first installed:

- **Size of file in bytes is greater than '?'**
- **Category name is '?'**
- **Mime type is '?'**
- **Size of the file in bytes is less than '?'**
- **Node name contains '?'**
- **Always (value is ignored)**

- **Any additional node attribute value is '?'**
- **Non-specific attribute ? value is ?**
- **Attribute ? value is ?**
- **Node assigned Classifications '?'**
- **Primary RM Classification '?'**
- **RM Essential '?'**
- **Security Clearance Level '?'**
- **Supplemental Markings '?'**
- **OR '?'**
- **AND '?'**
- **NOT '?'**
- **Project '?'**
- **Volume '?'**
- **Creation/Modification Date '?'**
- **Newest Version '?'**
- **RM Status '?'**
- **Object type in ?**
- **Stored below ?**
- **Stored below Container Type ?**
- **Stored in Personal Workspace (value is ignored)**
- **All Thumbnails**
- **Volume Free Space (MB)**

Note: When no rules are defined, the only icon that appears in the **Modify** column of the **Configure Storage Rules** page is the **Add** icon.

Additional rules are installed by Content Server optional modules:

- Controlled Viewing and Printing
- Enterprise Library

For more information, see "Available Storage Rules" on page 388 and "Examples Showing How to Define Storage Rules" on page 396.

25.3.1 Available Storage Rules

This page lists the storage rules available in Content Server. When a Document has the value you define assigned to it, that Document will be stored in the Storage Provider specified in the rule. You can find examples detailing many of these storage rules in “Examples Showing How to Define Storage Rules” on page 396.

Default Storage Rules

The following storage rules are available by default when you install Content Server:

Note: Content Move also makes the logical operators `AND`, `OR` and `NOT` available, which allow you to create complex rules.

Size of file in bytes is greater than '?'

- **Description**: if a Document's file size exceeds the file size stipulated in this rule, that Document will be stored in the Storage Provider specified in the rule.
- **Value Represented by** '?': <*file_size*> in bytes. For example, to represent 100 KB, type “1048576”.
- **Syntax**: `Size of file in bytes is greater than '1048576'`

Category name is '?'

- **Description**: if a Document has the specified Category assigned to it, that Document will be stored in the Storage Provider specified in the rule.
- **Value Represented by** '?': <*category_name*>. An example of a Category name is “myCategory”.
- **Syntax**: `Category name is 'myCategory'`

Mime Type is '?'

- **Description**: if a Document is of the specified MIME type, that Document will be stored in the Storage Provider specified in the rule.
- **Value Represented by** '?': <*MIME_type_name*>. An example of a MIME type name is “application/msword”.
- **Syntax**: `Mime Type is 'application/msword'`

Size of file in bytes is less than '?'

- **Description**: if a Document's file size is less than the file size stipulated in this rule, that Document will be stored in the Storage Provider specified in the rule.
- **Value Represented by** '?': <*file_size*> in bytes. For example, to represent 100 KB, type “1048576”.
- **Syntax**: `Size of file in bytes is less than '1048576'`

Node name contains '?'

- **Description**: if a Document's node name contains the specified string, that Document will be stored in the Storage Provider specified in the rule. Enter any string which can be part of the node name.
- **Value Represented by '?'**: <*node_name*>. An example of a Node name is “test”.
- **Syntax**: `Node name contains 'test'`

Always (value is ignored)

- **Description**: OpenText does not recommend that you use this storage rule, as it applies to *any* object type. An arbitrary value has to be entered.

Any additional node attribute value is '?'

- **Description**: if a Document has an additonal node attribute, and that additional node attribute contains the specified string, that Document will be stored in the Storage Provider specified in the rule. Enter any string which can be part of the node attribute value.

  This rule applies to *additional* node attributes which can be defined on the **Administering Additional Node Attributes** administration page. For more information, see *OpenText Content Server - Category and Attribute Administration (LLESWAT-AGD)*.
- **Value Represented by '?'**: <*node_attribute_value*>. An example of a node attribute value is “test”.
- **Syntax**: `Any additional node attribute value is 'test'`

Non-specific attribute ? value is ?

- **Description**: if a Document has a named, but unspecified, Category attribute that contains the specified string, that Document will be stored in the Storage Provider specified in the rule. *The Category attribute does not need to be specified*.
- **Value Represented by the first ?**: <*category_name*>.<*attribute_name*>. An example of a Category name and an Attribute name is “myCategory.myAttr”.
- **Value Represented by the second ?**: <*attribute_value*>. An example of an attribute value is “anyValue”.
- **Syntax**: `Non-specific attribute myCategory.myAttr value is anyValue`

Attribute ? value is ?

- **Description**: if a Document has a named and specified Category attribute that contains the specified string, that Document will be stored in the Storage Provider specified in the rule. *The Category attribute needs to be specified*. This storage rule is available because attributes can have multiple values.
- **Value Represented by the first ?**: <*category_name*>[<*x*>].<*attribute_name*>[<*z*>], where <*x*> and <*z*> are positive integers representing the specific Category and

the specific attribute. An example that references the third row of the attribute *myAttr* in the Category *myCategory* is: “myCategory[1].myAttr[3]”.

Tip: Because there is always only one row in the Category, <*x*> will always be 1, and must always be included.

Note: If the Category contains the *Set* attribute, and you want to specify a value within that Set, you need to represent the Category in this form: <*category_name*>[<*x*>].<*set_name*>[<*y*>].<*attribute_name*>[<*z*>]

An example that references the third row of an attribute named *myAttr*, in the fourth row of a set named *mySet*, in the category named *myCategory* is: “myCategory[1].mySet[4].myAttr[3]”.

- **Value Represented by the second ?**: <*attribute_value*>. An example of an attribute value is “anyValue”.
- **Syntax without Set**: `Attribute myCategory[1].myAttr[3] value is anyValue`
- **Syntax with Set**: `Attribute myCategory[1].mySet[4].myAttr[2] value is anyValue`

Node assigned Classifications

- **Description**: If a document has the specified Classification, Records Management Classification, Records Management Folder, or Provenance assigned to it, that document will be stored in the Storage Provider specified in the rule. The rule applies to both primary and secondary RM Classifications and RM Folders.
- **Value**: <*Classification path*>. Select a Classification, Records Management Classification, Records Management Folder, or Provenance value in the Browse Classifications or My Classifications Favorites window.
- **Syntax**: `Classification:`*`<Classification Name, RM Classification name, RM Folder name, or Provenance>`*

Primary RM Classification '?'

- **Description**: this rule checks if a Document has a specific Records Management Classification assigned to it. If so, that Document will be stored in the Storage Provider specified in the rule.
- **Value**: the Records Management Classification name. Browse the classification tree and select a value.
- **Syntax**: `RM Classification '`*`<RM_classification_name>`*`'`

RM Essential '?'

- **Description**: this rule checks if a Document has a specific Records Management Essential value assigned to it. If so, that Document will be stored in the Storage Provider specified in the rule.
- **Value**: the Records Management Essential value. Select an Essential value from the list.

- **Syntax**: `RM Essential '<RM_essential_value>'`

Security Clearance Level '?'

- **Description**: this rule checks if a Document has a specific Security Clearance level assigned to it. If so, that Document will be stored in the Storage Provider specified in the rule.

  The rule applies specifically to the chosen Security Level; it does not apply to items with a Security Level below the chosen level. If there are several levels, it can be necessary to concatenate one or more security clearance rules.

  You can only edit rules that use Security Levels for which you have the *See* permission. If existing rules use Security Levels for which you do not have the *See* permission, you will see that the rules exist but you cannot access them. Documents that have their Security Levels updated will be placed in the queue and reevaluated by the rule.
- **Value**: a Security Clearance level. Select a Security Clearance level from the list. Only Security Clearance levels for which you have the *See* permission are displayed in the list.
- **Syntax**: `Security Clearance Level '<SC_level>'`

Supplemental Markings '?'

- **Description**: this rule checks if a Document has specified Security Clearance supplemental marking(s) assigned to it. If so, that Document will be stored in the Storage Provider specified in the rule.

  You can only edit rules that use Supplemental Markings for which you have the *See* permission. If existing rules use Security Levels for which you do not have the *See* permission, you will see that the rules exist but you cannot access them. Documents that have their Supplemental Markings updated will be placed in the queue and reevaluated by the rule.
- **Value**: a Security Clearance supplemental marking. Select one or more supplemental marking(s) from the list. Only Supplemental Markings for which you have the *See* permission are displayed in the list.
- **Syntax**: `Supplemental Markings '<SC_supplemental_marking(s)>'`

OR '?'

- **Description**: This rule selects from several rules with the `OR` operator.
- **Value**: `Description, Rule, Value`. For details, see "To Combine Several Rules with AND, OR Operators" on page 395.

AND '?'

- **Description**: This rule combines several rules with the `AND` operator.
- **Value**: `Description, Rule, Value`. For details, see "To Combine Several Rules with AND, OR Operators" on page 395.

NOT '?'

- **Description**: This rule excludes all content to which the rule does not apply
- **Value**: `Rule, Value`.

Project '?'

- **Description**: This rule checks if a document is assigned to a specific project, that you select from a list. If so, that document will be stored in the Storage Provider specified in the rule.
- **Value**: the Node name of the Project.
- **Syntax**: `Project '`*`<project_node_name>`*`'`

Volume '?'

- **Description**: this rule checks if a document is stored in a specific Volume. If so, that document will be stored in the Storage Provider specified in the rule.
- **Value**: select a Volume from the list. An example of a Volume is: `Admin Home`.
- **Syntax**: `Volume 'Admin Home'`

Creation/Modification Date '?'

- **Description**: This rule checks the creation date of the document, or the modification date of the document, if one exists. If the creation date, or modification date, of the document is equal to the date specified in the rule, that document will be stored in the Storage Provider specified in the rule.

  You can optionally select a time range, one of: earlier, later, equal, between, exactly, more, or less.
- **Value**: a date value of the form DD/MM/YYYY. An example is “28/02/2014”.

  Tip: Select the year first, then the current date is preset.
- **Syntax**: `Creation/Modification Date '28/02/2014'`

Newest Version '?'

- **Description**: If the rule is set to TRUE, the latest version or rendition of the document will be stored in the Storage Provider specified in the rule. If the rule is set to `FALSE`, all versions and renditions *except* the newest version or rendition will be stored in the Storage Provider specified in the rule.
- **Value**: `TRUE` or `FALSE`
- **Syntax**: `Newest Version 'TRUE'` or `Newest Version 'FALSE'`

RM Status '?'

- **Description**: this rule checks if a Document has a specific Records Management Status code assigned to it. If so, that Document will be stored in the Storage Provider specified in the rule.
- **Value**: <*Status Code*>. Select an RM Status code value from the list.
- **Syntax**: `RM Status '<RM_status_code>'`

Object Type in ?

- **Description**: This rule checks if a document has a specific object type assigned. If so, that document will be stored in the Storage Provider specified in the rule. You can select one or more types.

  OpenText recommends that you only select types with content.
- **Value**: an object type, which type has content, that you select from the list. Examples of types with content include: `144`, `753`, `825`.
- **Syntax**: `Object Type in 144`

Stored below ?

- **Description**: This rule checks if a document is stored in a specific Container, that you select from a list. If so, that document will be stored in the Storage Provider specified in the rule.
- **Value**: the node name of the Container.
- **Syntax**: `Stored below <container_node_name>`

Stored below Container Type ?

- **Description**: This rule checks if a document is stored in a specified Container type, that you select from a list. If so, that document will be stored in the Storage Provider specified in the rule. You can select one or more types.
- **Value**: the Container type.
- **Syntax**: `Stored below Container Type <container_type>`

Stored in Personal Workspace (value is ignored)

- **Description**: This rule checks if a document is stored in a Personal Workspace. If so, that document will be stored in the Storage Provider specified in the rule.
- **Value**: Null, nothing has to be entered.
- **Syntax**: `Stored in Personal Workspace (value is ignored)`

All Thumbnails

- **Description**: This rule routes Thumbnails to the designated Logical Storage Provider.

- **Value**: No value is required.

Volume Free Space (MB)

- **Description**: this rule checks the remaining free space available on the volume on which Content Server is attempting to store the Document. If the free space will be less than the configured free space value specified in the rule, it will indicate that the Document cannot be stored on the volume. Content Server will then try the next volume in the list until it can save the Document. If the Document cannot be saved to any volume, it will be stored in the default volume.
- **Value**: a numeric value, in MB, needs to be entered. An example is “500”.

25.3.2 To Define a Storage Provider Rule

To define a Storage Provider rule:

1. In the **Storage Provider Settings** area of the Content Server Administration page, click the **Configure Storage Rules** link.

2. On the **Configure Storage Rules** page, in the **Storage Rules** area, under the **Modify** column, click the **Add new rule before this one** icon, ✚.

   The new rule will appear above the current rule.

3. On the **Add New Rule** page, from the **Rule** list, select a rule.

4. In the **Value** field, type a rule value.

5. Optional In the **Description** field, type a description of your new rule.

   Note: Although the **Description** field is optional, OpenText recommends that you always enter a description when creating a new Storage Rule.

6. The next fields available to you will be determined by the rule you selected in Step 3. If your new rule contained a variable, indicated by ?, you will need to type a value for that variable. These fields are mandatory.

   a. In the **Value** field, type the value you want to define this rule.

   b. In the **Attribute Specification** field, type a value for the attribute specification you want set for this rule.

   c. In the **Attribute Value** field, type a value for the attribute you want set for this rule.

7. From the **Logical Storage Provider** list, click the Storage Provider you want associated with the rule.

8. Click **Submit**.

25.3.3 To Combine Several Rules with AND, OR Operators

To combine several rules with AND, OR operators:

Generally, all defined rules are processed in the order of their definition and, if any rule applies, the content is moved to the storage provider assigned to the rule. This corresponds with an OR operator. The rule operators AND and OR provided with the Content Move functionality allow you to combine several rules to define a more complex evaluation. For instance, you can make the content move dependent on a certain file size and type, or on an attribute value or a modification date.

1. On the Content Server Administration page, in the **Storage Provider Settings** area, click the **Configure Storage Rules** link.
2. On the **Configure Storage Rules** page, click the **Add new rule before this one** icon, ✚ for the expression you want the new rule to appear above in the list.
3. Select the type of Rule you want to define (`AND`, `OR`).
4. Define a **Description** for the rule, which will appear in the overview on the `Configure Storage Rules` page.
5. In the `Value` section, define the first rule.
6. Click on Apply this value ( ) to apply the rule before defining the next rule in the combination set.
7. Define the next rule that you want to combine with the previous one. Again, the order of the rules is significant. Therefore, you find an Add icon behind each rule in the combination set. Click on the appropriate Add ( ) icon, depending on which expression you want the new rule to appear above in the set.
8. From the **Logical Storage Provider** list, click the Storage Provider you want associated with the rule.
9. Click **Submit**.

25.3.4 To Edit a Storage Provider Rule

To edit a Storage Provider rule:

1. In the **Storage Provider Settings** area of the Content Server Administration page, click the **Configure Storage Rules** link.
2. On the **Configure Storage Rules** page, click the **Edit** icon, ✎, next to the storage rule you want to edit.
3. On the **Configure Rule** page, change any of the available parameters.
4. Click **Submit**.

25.3.5 To Delete a Storage Provider Rule

To delete a Storage Provider rule:

1. In the **Storage Provider Settings** area of the Content Server Administration page, click the **Configure Storage Rules** link.

2. On the **Configure Storage Rules** page, click the **Delete** icon, ⊟, next to the rule you want to delete.

25.3.6 To Change the Order of a Storage Provider Rule

To change the order of a Storage Provider rule:

1. In the **Storage Provider Settings** area of the Content Server Administration page, click the **Configure Storage Rules** link.

2. On the **Configure Storage Rules** page, click the **Up**, ⇧, or **Down** icon, ⇩, for a rule until it reaches the position you want in the list.

25.3.7 Examples Showing How to Define Storage Rules

Below are examples demonstrating how to set some of the available storage rules. Before beginning any of the examples below, you must first:

1. On the Content Server Administration page, under **Storage Provider Settings**, select **Configure Storage Rules**.
2. On the **Configure Storage Rules** page, in the **Storage Rules** area, under the **Modify** column, click the **Add new rule before this one** button. This brings you to the **Add New Rule** page.

Examples for the Storage Rules Available by Default

These examples demonstrate how to set the storage rules available by default when you install Content Server

➡ **Example 25-1: Category name is '?'**

If you want all Documents that have been assigned the Category “Purchasing” added to a storage provider you specify:

1. From the **Rule** list, select **Category name is** '**?**'.
2. In the **Description** field, type “Documents that have been assigned the *Purchasing* Category will be stored in the specified Logical Storage Provider.”
3. In the **Value** field, type: Purchasing
4. From the **Logical Storage Provider** list, select the storage provider that you want used to store this Document if this condition is met.

5. Click **Submit**.

Example 25-2: Mime type is '?'

If you want all Documents of the Mime type “application/msword” added to a storage provider you specify:

1. From the **Rule** list, select **Mime type is** '**?**'.
2. In the **Description** field, type “Documents with Mime type 'application/msword' will be stored in the specified Logical Storage Provider.”
3. In the **Value** field, type: application/msword
4. From the **Logical Storage Provider** list, select the storage provider that you want used to store this Document if this condition is met.
5. Click **Submit**.

Example 25-3: Node name contains '?'

If you want all Documents with a node name that contains the string “xyz” added to a storage provider you specify:

1. From the **Rule** list, select **Node name contains** '**?**'.
2. In the **Description** field, type “Documents with a node name that contains the string ‘xyz’ will be stored in the specified Logical Storage Provider.”
3. In the **Value** field, type: xyz
4. From the **Logical Storage Provider** list, select the storage provider that you want used to store this Document if this condition is met.
5. Click **Submit**.

Example 25-4: Any additional node attribute value is '?'

If you want all Documents whose additional node attribute value contains the string “xyz” added to a storage provider you specify:

1. From the **Rule** list, select **Any additional node attribute value is** '**?**'.
2. In the **Description** field, type “Documents whose additional node attribute value contains the string ‘xyz’ will be stored in the specified Logical Storage Provider.”
3. In the **Value** field, type: xyz
4. From the **Logical Storage Provider** list, select the storage provider that you want used to store this Document if this condition is met.
5. Click **Submit**.

Example 25-5: Non-specific attribute ? value is ?

If you want all Documents that:

- have a specific Category assigned to them, and
- which Category has a named, but not specified Attribute, and
- which Attribute has a specific value assigned to it,

added to a storage provider you specify:

1. From the **Rule** list, select **Non-specific attribute ? value is ?**.
2. In the **Description** field, type “Documents assigned a Category named ‘myCategory’, that has an Attribute named ‘myAttr’, which Attribute has the assigned value ‘anyValue’, will be stored in the specified Logical Storage Provider.”
3. In the **Attribute Specification** field type the Category and the Attribute: myCategory.myAttr
4. In the **Attribute Value** field, type the value of the Attribute: anyValue
5. From the **Logical Storage Provider** list, select the storage provider that you want used to store this Document if this condition is met.
6. Click **Submit**.

Example 25-6: Attribute ? value is ? (without Set)

If you want all Documents that:

- have a specific Category assigned to them, and
- which Category has a named and specified Attribute, and
- which Attribute has a specific value assigned to it,

added to a storage provider you specify:

1. From the **Rule** list, select **Attribute ? value is ?**.
2. In the **Description** field, type “Documents assigned a Category named ‘myCategory’, that has a specific Attribute named ‘myAttr’, which Attribute has the assigned value ‘anyValue’, will be stored in the specified Logical Storage Provider.”
3. In the **Attribute Specification** field type the Category and the *specific* Attribute: myCategory[1].myAttr[3]
4. In the **Attribute Value** field, type the value of the Attribute: anyValue
5. From the **Logical Storage Provider** list, select the storage provider that you want used to store this Document if this condition is met.

6. Click **Submit**.

Example 25-7: Attribute ? value is ? (with Set)

If you want all Documents that:

- have a specific Category assigned to them, and
- which Category has a Set, and
- which Set has a specific value assigned to a named attribute

added to a storage provider you specify:

1. From the **Rule** list, select **Attribute ? value is ?**.
2. In the **Description** field, type “Documents assigned a Category named ‘myCategory’, with a Set called ‘mySet’, which Set has a specific Attribute named ‘myAttr’, which Attribute has the assigned value ‘anyValue’, will be stored in the specified Logical Storage Provider.”
3. In the **Attribute Specification** field type the Category and the *specific* Attribute: myCategory[1].mySet[4].myAttr[3]
4. In the **Attribute Value** field, type the value of the Attribute: anyValue
5. From the **Logical Storage Provider** list, select the storage provider that you want used to store this Document if this condition is met.
6. Click **Submit**.

Example 25-8: Primary RM Classification '?'

If you want all Documents with a specific Records Management Classification assigned to them added to a storage provider you specify:

1. From the **Rule** list, select **RM Classification** '**?**'.
2. In the **Description** field, type “Documents with the RM Classification ‘xyz’ assigned to them will be stored in the specified Logical Storage Provider.”
3. In the **Value** field, browse the Classification tree and select a Classification.
4. From the **Logical Storage Provider** list, select the storage provider that you want used to store this Document if this condition is met.
5. Click **Submit**.

Example 25-9: RM Essential '?'

If you want all Documents with a specific Records Management Essential value assigned to them added to a storage provider you specify:

1. From the **Rule** list, select **RM Essential** '**?**'.
2. In the **Description** field, type “Documents with the RM Essential value ‘xyz’ assigned to them will be stored in the specified Logical Storage Provider.”
3. In the **Value** field, select an Essential value from the list.
4. From the **Logical Storage Provider** list, select the storage provider that you want used to store this Document if this condition is met.
5. Click **Submit**.

Example 25-10: Security Clearance Level '?'

If you want all Documents with a specific Security Clearance level assigned to them added to a storage provider you specify:

1. From the **Rule** list, select **Security Clearance Level** '**?**'.
2. In the **Description** field, type “Documents with the Security Clearance level ‘xyz’ assigned to them will be stored in the specified Logical Storage Provider.”
3. In the **Value** field, select a Security Clearance level from the list.
4. From the **Logical Storage Provider** list, select the storage provider that you want used to store this Document if this condition is met.
5. Click **Submit**.

Example 25-11: Supplemental Markings '?'

If you want all Documents with specified Security Clearance supplemental marking(s) assigned to them added to a storage provider you specify:

1. From the **Rule** list, select **Supplemental Markings** '**?**'.
2. In the **Description** field, type “Documents with the Security Clearance supplemental marking(s) ‘xyz’ assigned to them will be stored in the specified Logical Storage Provider.”
3. In the **Value** field, select one or more supplemental marking(s) from the list.
4. From the **Logical Storage Provider** list, select the storage provider that you want used to store this Document if this condition is met.
5. Click **Submit**.

Example 25-12: Project '?'

If you want all Documents assigned to a specific Project added to a storage provider you specify:

1. From the **Rule** list, select **Project** '**?**'.
2. In the **Description** field, type “All Documents assigned to the ‘xyz’ Project will be stored in the specified Logical Storage Provider.”
3. In the **Value** field, from the list, select the Project.
4. From the **Logical Storage Provider** list, select the Storage Provider that you want used to store this Document if this condition is met.
5. Click **Submit**.

Example 25-13: Volume '?'

If you want all Documents stored in a specific Volume added to a storage provider you specify:

1. From the **Rule** list, select **Volume** '**?**'.
2. In the **Description** field, type “Documents stored in the Volume ‘xyz’ will be stored in the specified Logical Storage Provider.”
3. In the **Value** field, from the list, select a Volume.
4. From the **Logical Storage Provider** list, select the Storage Provider that you want used to store this Document if this condition is met.
5. Click **Submit**.

Example 25-14: Creation/Modification Date '?'

If you want all Documents created or modified before, on or after a specified date added to a storage provider you specify:

1. From the **Rule** list, select **Creation/Modification Date** '**?**'.
2. In the **Description** field, type “Documents created or modified before/on/after ‘DD/MM/YYYY’ will be stored in the specified Logical Storage Provider.”
3. In the **Value** field, type a date in the form DD/MM/YYYY.

   Select a time range, one of: earlier, later, equal, between, exactly, more, or less.
4. From the **Logical Storage Provider** list, select the Storage Provider that you want used to store this Document if this condition is met.
5. Click **Submit**.

Example 25-15: Newest Version '?'

If you want the latest version or rendition of Documents added to a storage provider you specify:

1. From the **Rule** list, select **Newest Version** '**?**'.
2. In the **Description** field, type “The latest version or rendition of Documents will be stored in the specified Logical Storage Provider.”
3. In the **Value** field, select “TRUE”.
4. From the **Logical Storage Provider** list, select the Storage Provider that you want used to store this Document if this condition is met.
5. Click **Submit**.

Example 25-16: RM Status '?'

If you want all Documents with a specific Records Management Status code assigned to them added to a storage provider you specify:

1. From the **Rule** list, select **RM Status** '**?**'.
2. In the **Description** field, type “Documents with the RM Status code ‘xyz’ assigned to them will be stored in the specified Logical Storage Provider.”
3. In the **Value** field, type an RM Status code.
4. From the **Logical Storage Provider** list, select the storage provider that you want used to store this Document if this condition is met.
5. Click **Submit**.

Example 25-17: Object Type in ?

If you want all Documents with a specific object type assigned added to a storage provider you specify:

1. From the **Rule** list, select **Object Type in ?**.
2. In the **Description** field, type “Documents with the object type ‘xyz’ assigned to them will be stored in the specified Logical Storage Provider.”
3. In the **Value** field, from the list, select all object type(s) to which you want this rule applied. OpenText recommends that you select type(s) that have content.
4. From the **Logical Storage Provider** list, select the Storage Provider that you want used to store this Document if this condition is met.
5. Click **Submit**.

Example 25-18: Stored below ?

If you want all Documents stored in a specified Container added to a storage provider you specify:

1. From the **Rule** list, select **Stored below ?**.
2. In the **Description** field, type “Documents stored in Container ‘xyz’ will be stored in the specified Logical Storage Provider.”
3. In the **Value** field, select the container node name.
4. From the **Logical Storage Provider** list, select the Storage Provider that you want used to store this Document if this condition is met.
5. Click **Submit**.

Example 25-19: Stored below Container Type ?

If you want all Documents stored in a specified Container type added to a storage provider you specify:

1. From the **Rule** list, select **Stored below Container Type ?**.
2. In the **Description** field, type “Documents stored in Container type ‘xyz’ will be stored in the specified Logical Storage Provider.”
3. In the **Value** field, from the list, select one or more container types.
4. From the **Logical Storage Provider** list, select the Storage Provider that you want used to store this Document if this condition is met.
5. Click **Submit**.

Example 25-20: Stored in Personal Workspace (value is ignored)

If you want all Documents stored in a Personal Workspace added to a storage provider you specify:

1. From the **Rule** list, select **Stored in Personal Workspace (value is ignored)**.
2. In the **Description** field, type “Documents stored in a Personal Workspace will be stored in the specified Logical Storage Provider.”
3. Nothing needs to be entered to the **Value** field.
4. From the **Logical Storage Provider** list, select the Storage Provider that you want used to store this Document if this condition is met.
5. Click **Submit**.

Example 25-21: Volume Free Space (MB)

If, before storing a Document, you want Content Server to assess the free space available on the volume and only store to a volume that has 500 MB of free space available:

1. From the **Rule** list, select **Volume Free Space (MB)**.

2. In the **Description** field, type “Skip if less than 500 MB free.”
3. In the **Volume Free Space (MB)** field, type: 500
4. From the **Logical Storage Provider** list, select the storage provider that you want Content Server to assess first when storing this Document.
5. Click **Submit**.

Chapter 26

Recycle Bin Administration

By default, Content Server is installed with the Recycle Bin enabled, so that an item that has been deleted can be restored to Content Server.

When a user deletes an item, Content Server places the item in the Recycle Bin. The Recycle Bin allows any user that could delete the item from its original location to restore the item or purge it from the Recycle Bin. Items that are purged from the Recycle Bin are permanently deleted.

Not every item type can be restored after it is deleted. Content Server is capable of restoring a wide variety of deleted item types, but certain *non-restorable* item types are not placed in the Recycle Bin when they are deleted. Some item types can be configured as restorable or non-restorable. For more information, see "Restorable and Non-restorable Item Types" on page 408.

Note: If you do not want the Recycle Bin to be available to Content Server users and administrators, you can disable it. See "Disabling the Recycle Bin" on page 409.

26.1 The Recycle Bin Manager Usage Privilege

As an administrator, you can assign any Content Server user to the role of Recycle Bin Manager. Making a user a Recycle Bin Manager allows you to delegate the work of purging and restoring items from the Recycle Bin without assigning a user the `System administration rights` privilege.

A Recycle Bin Manager is a user that can view, restore, and purge any of the items in the Recycle Bin, regardless of the user that deleted them, including items that the Recycle Bin Manager could not have accessed in their original location (and cannot access after they have been restored). A Recycle Bin Manager can access the Recycle Bin even if you have disabled user access to the Recycle Bin (see "User Options" on page 410).

To add and remove users from the Recycle Bin Manager group, open the **Administer Usage Privileges** administration page and, beside **Recycle Bin Administration**, click **Edit Restrictions**. To make a user a Recycle Bin Manager, add the user to the **Recycle Bin Manager** group.

By default, the **Recycle Bin Administration** usage privilege is restricted and is not assigned to any user. For more information on object and usage privileges, see "Administering Object Privileges and Usage Privileges" on page 343.

26.2 Restoring and Purging Deleted Items

When a restorable item is deleted, it is placed in the Recycle Bin. Items in the Recycle Bin can be restored to their original location in Content Server. They can also be purged, either automatically or manually.

26.2.1 Accessing the Recycle Bin

To view the items in the Recycle Bin, click **Recycle Bin** on the **Tools** global menu.

By default, the Recycle Bin has columns that show the type, name and size of each deleted item, the user who deleted it, the date it was deleted, and its location at the time it was deleted. If you have enabled the **Display purge date column in Recycle Bin** setting in the Recycle Bin user options (see "User Options" on page 410), it also displays the date that an item is scheduled to be purged automatically. To locate items in the Recycle Bin, you can use the content filter or the default Recycle Bin views (**I Deleted Today**, **I Deleted**, **Anyone Deleted Today** or **Anyone Deleted**).

A deleted container appears in the Recycle Bin with a number in the **Size** column that indicates the number of child items that were in it. Child items of a container do not appear in the Recycle Bin if the parent container has been deleted. To restore one or more of the items that were in the container at the time of deletion, you must restore the container. When you restore a container, it is restored along with the items that it contained at the time of deletion.

If you restore a deleted item or container, it is restored to its original location.

Note: Items that were deleted from a container before the container was deleted are not restored when the container is restored. After the container is restored, they remain in the Recycle Bin. If the container is restored, such items become visible in the Recycle Bin and can be restored explicitly.

Restoring Deleted Items

To restore documents from the Recycle Bin:

1. Click **Recycle Bin** on the **Tools** global menu. The **Recycle Bin** page appears.
2. Select one or more items that you want to restore. If the item that you want to restore resided in a Content Server container that has been deleted, select the Content Server container to restore it and all of the sub-items that it contained at the time of its deletion.

   Tip: Use the Content Filter or the Recycle Bin views to assist you in locating items to restore.
3. Click **Restore**, and then confirm the restore operation.

The items that you selected are restored. The **Status** on the confirmation page notes the location that they were restored to.

Purging Deleted Items

Purging can be done automatically or manually. When you purge an item from the Recycle Bin, the item is permanently removed from Content Server. For the settings governing automatic purges see “Automatic Purge Settings” on page 409.

To manually purge documents in the Recycle Bin:

1. Click **Recycle Bin** on the **Tools** global menu. The **Recycle Bin** page appears.
2. Select one or more items that you want to purge. If the item that you want to purge resided in a Content Server container that has been deleted, select the Content Server container to purge it and all of the sub-items that it contained at the time of its deletion.

   Tip: Use the Content Filter or the Recycle Bin views to assist you in locating items to purge.

3. Click **Purge**, and then confirm the purge operation.

The items that you selected are purged. Purged items are deleted permanently and cannot be restored.

26.2.2 Accessing Legacy Recycled or Deleted Items

If you have upgraded to Content Server 16 or later from Content Server 10.5 or earlier and your previous version made use of Undelete or the optional Recycle Bin module, an additional **Legacy Recycled Items** or **Legacy Deleted Items** link appears below the default Recycle Bin views. The link is visible if you have `System administration rights` privilege or the Recycle Bin Manager usage privilege. It provides access to items that were in the Recycle Bin or Undelete Volume at the time that Content Server was upgraded to Content Server 16 or later.

Note: Items from the Undelete Volume have a different appearance in Content Server 16 and later. They are prefaced with the data ID of the item. A document that appeared in the Undelete Volume as `MyDocument.pdf`, for example, may appear in Content Server 16 as `[1234] MyDocument.pdf`.

To restore a legacy recycled or deleted item, move it to a place that is accessible to the user who wants to regain access to the item. Adjust the item’s permissions, if necessary, so that the user can access it.

Tip: A user with the Recycle Bin Manager usage privilege can restore a legacy recycled or deleted item that they otherwise do not have permission to access. Consequently, it is possible for a Recycle Bin Manager to restore an item and be unable to access it after it is restored, even if it is restored to a location that the Recycle Bin Manager can access, such as the Recycle Bin Manager’s personal workspace.

When you restore a legacy recycled or deleted item, you can specify the location to restore it to. To ensure that a user can regain use of a restored legacy recycled or deleted item, OpenText recommends that the Recycle Bin Manager restore the item directly to a folder that both the user and the Recycle Bin Manager can access.

If you decide that you no longer require access to legacy recycled or deleted items, you can purge them. Select one or more items in the legacy items folder and then click **Purge**. Items that are purged are immediately deleted. They are not placed in the Recycle Bin. Once you delete all of the items from the legacy items folder, the link to it no longer appears in the Recycle Bin.

26.3 Configuring Recycle Bin

On the **Recycle Bin Settings** page, you can configure the behavior and appearance of the Recycle Bin. There are three main sections: **Supported Types**, **Settings** and **User Options**

If you have upgraded to Content Server 16 or later from Content Server 10.5 or earlier and your previous version made use of Undelete or the optional Recycle Bin module, an additional link appears at the top of the page: **Manage Legacy Deleted Items**. Click this link to access items that were in the Recycle Bin or Undelete Volume at the time that Content Server was upgraded to Content Server 16 or later.

26.3.1 Restorable and Non-restorable Item Types

Items that are restorable are placed in the Recycle Bin when they are deleted. They can be restored after deletion. Items that are non-restorable are purged immediately and cannot be restored. As an administrator, you can choose whether to make certain item types restorable or non-restorable.

Not every item type can be configured in this manner. Some Content Server item types can never be made restorable and some other Content Server item types are always restorable. The remaining item types are configurable. You can set them to restorable or non-restorable, according to your organization’s needs.

The **Recycle Bin Settings** page, in the **Supported Types** section provides information on item types. Use the links in this section to view listings of restorable and non-restorable item types and to configure eligible items.

Restorable Item Types

Click **Edit/Review Restorable Node Types** to view a listing of items that Content Server can restore. Item types that appear in the **Mandatory** section are always restorable. You cannot configure them. Item types that appear in the **Optional** section are configurable. If you enable one of the item types in this section, deleted items of that type are placed in the Recycle Bin. If you disable one of them, items of that type are purged immediately upon deletion and cannot be restored.

Note: Changes made on this page are not retroactive. They do not affect items that are already in the Recycle Bin.

Non-restorable Item Types

Click **Review Restorable Node Types** to view a listing of item types that Content Server cannot restore. These item types can never be made restorable.

26.3.2 Settings

The **Settings** section of the **Recycle Bin Settings** page allows you to enable or disable the Recycle Bin and configure settings that govern the automatic purging of items in the Recycle Bin.

Disabling the Recycle Bin

You can disable the Recycle Bin in your Content Server deployment. If you do, deleted items cannot be restored. They are scheduled for purge immediately upon deletion.

To disable the Recycle Bin

1. On the Content Server Administration page, in the **System Administration** section, click **Recycle Bin**.

2. On the **Recycle Bin Settings** page, in the **Enable** section, select **Schedule immediate purge of all items when they are deleted**.

3. Click **Save Changes**.

Automatic Purge Settings

To retain deleted items in the Recycle Bin until a user purges them, enable **Keep deleted items until manually purged**. To configure Content Server to automatically purge deleted items in the Recycle Bin after a period of time, enable **Purge items automatically** and specify a number of days in the box before `Days to retain before purging`.

If you want the Recycle Bin to display the date that Content Server is scheduled to purge an item from the Recycle Bin, enable **Display purge date column in Recycle Bin**. If this setting is enabled, the Recycle Bin displays a **Purge Date** column in addition to the columns that appear by default (**Type**, **Name**, **Size**, **Deleted By**, **Deleted Date**, and **Location**).

26.3.3 User Options

Recycle Bin user options govern whether Content Server users can access the Recycle Bin, its appearance if they can, and whether they can purge deleted items that are in the Recycle Bin.

To allow users access to the Recycle Bin, select **Ordinary users can see Recycle Bin**. If this setting is not selected, users do not have a **Recycle Bin** option in their **Tools** menu. If it is selected, the option does appear in their **Tools** menu and they can access the Recycle Bin to restore deleted items. To allow users to override automatic purge settings and purge deleted items themselves, select **Users can Purge items**.

User View Options enable filters that allow Content Server users to access items in the Recycle Bin. Disabling a filter prevents Content Server users from seeing and using it in the Recycle Bin. **User View Options** have no effect on users with the `System Administration rights` privilege. They do affect Recycle Bin Managers, unless you select **Recycle Bin Managers have full access to the Recycle Bin**.

To ensure that Recycle Bin Managers can access every Recycle Bin function, select **Recycle Bin Managers have full access to the Recycle Bin**.

Important

Enable at least one filter if you want Content Server users to have access to the Recycle Bin. Disabling every filter has the same effect as disabling **Ordinary users can see Recycle Bin**: it removes the **Recycle Bin** option from their **Tools** global menu.

Part 6

Module Administration

Chapter 27

Administering Modules

Content Server components are organized into core and optional software modules.

Core modules, such as Content Server Workspaces, Content Server Document Management, and Content Server Projects, are automatically installed when Content Server is installed. Optional modules, such as OpenText™ XML Workflow Extensions, are installed by a Content Server administrator during the initial installation of Content Server or afterwards. Optional modules extend the functionality of Content Server to meet your organization's specific needs. They may be new modules that you have purchased or modules that were available at the time of installation, but you chose not to install.

Tips

- For information on installing optional modules during a Content Server installation, see *OpenText Content Server - Installation Guide (LLESCOR-IGD)*.
- For additional information on installing, uninstalling and upgrading modules, see *OpenText Content Server - Module Installation and Upgrade Guide (LLESCOR-IMO)*.

27.1 Installing Modules

You install a module in two stages:

1. **Installation on the operating system**

   You configure your operating system to use the module, and install the module’s components into the `<Content_Server_home>/staging/` folder of your Content Server installation.
2. **Installation on Content Server**

   You use the Content Server Administration page to move the module from the `<Content_Server_home>/staging/` folder to the `<Content_Server_home>/module/` folder, and install it in Content Server,

After you complete the installation of a module on Content Server, you should also perform the following additional steps, as necessary:

Install Module Language Packs

If you run a multilingual deployment of Content Server, you should install a module language pack for each language in your Content Server deployment. Note, however, that some modules do not require language packs at all. For example, the Content Server Forms Workflow Designer module does not require a language pack. See “Creating, Installing and Upgrading Language Packs” on page 257.

Update the Content Server Help Indexes

Content Server modules make additions to the Content Server help files. After installing a module, you should update the User and Admin Online help. See "Updating the User and Admin Online Help" on page 422,

Apply Module Patches

Use Cluster Management or System Center Manager to ensure that your module patches are up to date. See *OpenText Content Server Cluster Management - OpenText Content Server (LLESPAT-AGD)* or *(SYSCM-AGD)*.

Review Audit Settings

The module that you install may add auditing events that you would like to enable. See "Administering Event Auditing" on page 319.

Apply a module license

Some modules need to be licensed. If the optional module that you are installing requires a license, obtain the license at http://productactivation.opentext.com/ContentServer and then apply the license file in OpenText Directory Services. See "Managing Licenses in Content Server" on page 247.

Note: This chapter explains how to configure Content Server interactively in two steps using a module installer and the Content Server Administration pages. You can also install Content Server modules automatically in a single step using OpenText™ System Center Manager. System Center Manager installs, configures, patches, and updates multiple OpenText software applications. For more information, see *OpenText System Center Manager - Installation and Configuration Guide (SYSCM-IGD)*.

27.1.1 Installing a Content Server Module on the Operating System

In the first stage of module installation, you install the module on the operating system.

Installing Modules on Windows

For Windows versions of Content Server modules, you perform the first stage of an installation using a Windows installer that allows you to select the Content Server instance that will run the module. The installer places the module's files in a subfolder of the `Content_Server_home\staging\` folder.

To install a module on Content Server running on Windows:

1. On the Content Server host computer, run the `<module_name>.exe` file to launch the module installer.

2. Advance past the **Welcome** and **License Agreement** dialog boxes.

3. Select the Content Server instance that will run the module, and then click **Next**.

> **Note:** If there is more than one Content Server instance on the host computer, each instance appears in the **Selection of install location** dialog box. You can select only one instance at a time.

4. Click **Install**.

   A progress indicator and status messages indicate the progression of the installation. When the installation is complete, a final dialog box appears.

5. Click **Finish** to exit the installer.

Installing Modules on Linux

For Linux versions of Content Server modules, you perform the first stage of an installation using a `.tar` compressed archive file. The extraction of this `.tar` file places the module's files in a subdirectory of the `Content_Server_home/staging/` directory.

To install a module on Content Server running on Linux:

1. Copy the module installation file to the <*Content_Server_home*> directory of your Content Server installation.

2. If the module installation file has a `.gz` file extension, expand it using gzip or another file compression program.

3. At the shell prompt, type the following command, and then press ENTER:

   ```
   tar -xvf <module_name>.tar
   ```

27.1.2 Installing a Module in Content Server

In a clustered instance of Content Server, perform the following procedure on each Content Server instance in your cluster.

> **Note:** When you install the same module on multiple instances of Content Server, you may see a **Missing software** error in the **Module Errors** section of the **Install Modules** page after you install the module on the first instance. This error indicates that your Content Server database contains information that pertains to this module, but your current instance does not yet have the module installed. Installing the module will resolve the error condition.

To install a module in Content Server:

1. In the **Installable Modules** section, select each of the modules that you want to install, and then click **Install**.

   > **Note:** When you enable a module that requires the installation of other modules, Content Server automatically selects the required modules if they have been installed on the operating system. Content Server can install numerous modules at once, but if you want to install the modules one at a time, install the required modules first.

2. Optional If a module that you are installing modifies the Content Server database, the **Content Server Database Upgrade Confirmation** page appears. Perform the following steps

   a. Click **Continue** to initiate the database upgrade.

   b. The **Restart Content Server** page appears. Click **Restart** to restart automatically, or click **Continue** if you prefer to restart Content Server using the operating system.

   c. Content Server displays **Restart Successful**. Click **Continue**.

   d. When the **Database Upgrade Status** page displays **The database upgrade has completed successfully**, click **Continue**.

   e. Content Server automatically restarts and you are returned to the **Database Upgrade Status** page. Click **Continue**.

3. The **Configure Modules** page appears. Click **Continue**. Content Server configures your modules.

4. Restart Content Server to commit the module configurations.

   a. The **Restart Content Server** page appears. Click **Restart** to restart automatically, or click **Continue** if you prefer to restart Content Server using the operating system.

   b. Content Server displays **Restart Successful**. Click **Continue**.

27.2 Configuring Modules

Modules are installed in two steps: installation and configuration. The **Configure Modules** page normally appears after you have successfully installed one or more modules (see “Installing Modules” on page 413). But you may need to open this page directly from the Content Server Administration page if you did not configure a module after you installed it. (For example, if you closed your browser before clicking **Continue** on the **Configure Modules** page.) Alternatively, OpenText Customer Support may ask you to visit the **Configure Modules** page while troubleshooting a module installation problem.

On the **Configure Modules** page, Content Server lists the **Modules To Be Configured**. Review the list and then click **Continue**. A progress bar indicates that Content Server is configuring the modules. When the **Restart Content Server** page appears, click **Restart** (or click **Continue** if you prefer to restart Content Server manually). After Content Server restarts, you are returned to the Content Server Administration page.

27.3 Uninstalling Modules

Content Server allows you to remove any optional module that you have installed.

Note: You can also remove certain pre-installed modules, such as Discussions, Projects, or Workflow. However, OpenText recommends that you do not uninstall pre-installed modules unless OpenText Customer Support instructs you to.

Content Server modules are uninstalled in two steps:

1. **Removal from Content Server**

   You use the Content Server Administration page to uninstall the module from Content Server and move its files from the `<Content_Server_home>/module/` folder to the `<Content_Server_home>/uninstalled/<yyyymmdd_hhmmss>/` folder.

   Tip: If you have previously modified or customized the module that you are uninstalling, the module version retained in the `/uninstalled/<yyyymmdd_hhmmss>/` folder includes your customizations. If you reinstall the module, you can use the version in the `/uninstalled/<yyyymmdd_hhmmss>/` folder, or download the released (unmodified) version of the module from OpenText My Support.

2. **Removal from the operating system**

   You remove module configuration information from your operating system, and delete the module files from the `<Content_Server_home>/uninstalled/<yyyymmdd_hhmmss>/` folder of your Content Server installation.

27.3.1 To View Uninstallable Modules

You can view a list of all Content Server modules that can be removed from your system and verify whether a module to be removed has dependent modules on the **View Uninstallable Modules** page.

To view uninstallable modules:

1. In the **Module Administration** section of the Administration page, click **View Uninstallable Modules**.

2. On the **View Uninstallable Modules** page, under the **Name** column, read through the list of Content Server modules which are available to be uninstalled from your system.

   If a module has an entry under the **Dependencies** column, the dependent module must be uninstalled first.

3. Once you have determined the modules you need to uninstall, see "Uninstalling a Content Server Module from Content Server" on page 418.

27.3.2 Uninstalling a Content Server Module from Content Server

In the first step of removing a Content Server module, you uninstall it using the Content Server **Uninstall Modules** administration page.

Note: Uninstalling a module from Content Server removes both the module and any associated language pack files. You do not need to perform an additional step to remove a module language pack.

To uninstall a module:

1. Open the Content Server Administration page.
2. On the Content Server Administration page, under **Module Administration**, click **Uninstall Modules**.
3. On the **Uninstall Modules** page, click **Uninstall** beside the module that you want to remove.

   Note: If a module is depended on by another module, it has no **Uninstall** button. You must uninstall every module listed in the **Dependencies** column before you can uninstall the module on which they depend.

   Content Server uninstalls the selected module, and then displays the **Restart Content Server** page. After you restart Content Server, the **Uninstall Modules** page appears again.

Removing the module from Content Server does not remove it from the operating system or file system, so it remains available for reinstallation. If you want, you can reinstall the module by moving the *<module_#_#_#>* file from the `<Content_Server_home>/uninstalled/<yyyymmdd_hhmmss>/` folder to the `<Content_Server_home>/staging/` folder and then by using the Content Server **Install Modules** administration page.

Notes

- Reinstalling a module as described above allows you to retain changes and customizations that you may have made to the module. If you have made changes, but would rather install the released version of the module, download it from OpenText My Support and install it normally.
- If you uninstall a module that has additional language files, the language files are retained. If you do not remove the module from the operating system, the language files will be reinstalled when you reinstall the module. However, if you remove the module from the operating system and then later reinstall it, you must install the module and the language pack separately.
- After you uninstall a module that has help files associated with it, update the Help index so that the module's help files are removed from the index. See "Updating the User and Admin Online Help" on page 422.

If you do not intend to reinstall the module, proceed to "Removing a Content Server Module from the Operating System" on page 419 for instructions on completely removing the module from the Content Server host computer.

27.3.3 Removing a Content Server Module from the Operating System

In the second step of removing a Content Server module, you remove the module from the operating system and file system. Follow the instructions in one of the following sections:

- "Removing a Content Server Module from Windows" on page 419
- "Removing a Content Server Module from Linux" on page 419

Removing a Content Server Module from Windows

To remove a module from Windows and the Windows file system, uninstall the module using Windows Add/Remove Programs.

To uninstall a Content Server module from Windows:

1. Open Control Panel, and then open Add/Remove Programs.
2. Select the module that you want to uninstall, and then click **Uninstall**.
3. After the uninstall software finishes running, open Windows Explorer and verify whether the module files remain in the `<Content_Server_home>/uninstalled/<yyyymmdd_hhmmss>/` folder. If necessary, delete the files manually.

Removing a Content Server Module from Linux

To remove a Content Server module from a Linux operating system and file system, delete the module files from the `<Content_Server_home>/uninstalled/<yyyymmdd_hhmmss>/` folder.

To delete the module files from a shell prompt, run the following command, logged on as the Content Server user:

```
rm -rf <Content_Server_home>\uninstalled
\<yyyymmdd_hhmmss><module_#_#_#>
```

27.4 Upgrading Modules

OpenText releases new versions of Content Server modules from time to time that you can download from OpenText My Support. OpenText recommends that you consult a module's Release Notes prior to beginning an upgrade installation.

A module is upgraded in two stages:

1. **Module Installation on the operating system**

   You configure your operating system to use the module, and install the module’s components into the *<Content_Server_home>*`/staging/` folder of your Content Server installation.
2. **Module Upgrade on Content Server**

   You use the Content Server Administration page to move the module from the *<Content_Server_home>*`/staging/` folder to the *<Content_Server_home>*`/module/` folder, and install it in Content Server.

The way you upgrade a module depends on the operating system that Content Server runs on. Once the new files are added to the appropriate locations in the *<Content_Server_home>*`/staging/` folder, the upgrade process is the same for Windows, and Linux operating systems.

Upgrading Modules on Windows or Linux

For Windows versions of Content Server modules, you perform the first stage of an upgrade using an InstallShield installation program. This installation program allows you to select the Content Server instance on which you want to upgrade the module and places the module's files in a subdirectory of the *<Content_Server_home>*`/staging/` directory.

For Linux versions of Content Server modules, you perform the first stage of an upgrade using a `.tar` compressed archive file. The extraction of this `.tar` file places the module's files in a subdirectory of the *<Content_Server_home>*`/staging/` directory.

Completing a Module Upgrade

You perform the second stage of a module upgrade using the **Upgrade Modules** administration page.

After you upgrade a module, the **Restart Content Server** page is the first page that appears in most cases. However, some module upgrades require you to set certain configuration parameters before restarting the server. For information about setting configuration parameters, see the module's specific documentation.

Notes

- If you have installed multiple modules, you will see them on the **Upgrade Modules** page. You can upgrade as many as nine modules at one time, as long as they have no dependencies on other modules. When a module has a dependency on another module, that module must first be added or upgraded.

- After you upgrade a module, update the help indexes so that changed content is available to be searched in the Online Help. For more information, see "Updating the User and Admin Online Help" on page 422.

27.4.1 To Upgrade Modules on Content Server Running on Windows

To upgrade modules on Content Server running on Windows:

1. Install the modules on Windows.

   - Download and run each module's installer.

     i. When the installer's **Welcome** dialog box appears, click **Next**.

     ii. On the **License Agreement** dialog box, accept the terms of the License Agreement, and then click **Next**.

     iii. In the **Selection of install location** dialog box, enable the Content Server instance on which you want the module installed, and then click **Next**.

     iv. Perform the installation. When the **Completing the Installation** dialog box appears, click **Finish**.

2. Upgrade the modules on Content Server.

   a. In the **Module Administration** section of the Content Server Administration page, click **Upgrade Modules**.

   b. On the **Upgrade Modules** page, enable the modules that you want to upgrade, and then click **Install**.

   The **Restart Content Server** page appears. After you restart Content Server, you are returned to the **Install Modules** page.

27.4.2 To Upgrade Modules on Content Server Running on Linux

To upgrade modules on Content Server running on Linux:

1. Install the modules on Linux.

   - Extract each module's installation file to the <*Content_Server_home*> directory.

     i. Copy the `<module_name>.tar` file to the <*Content_Server_home*> directory of the Content Server instance on which you want the module installed.

   - ii. At the shell prompt, type the following command, `tar -xvf <module_name>.tar`, and then press **ENTER**.

2. Upgrade the modules on Content Server.

   a. In the **Module Administration** section of the Content Server Administration page, click **Upgrade Modules**.

   b. On the **Upgrade Modules** page, enable the modules that you want to upgrade, and then click **Install**.

      The **Restart Content Server** page appears. After you restart Content Server, you are returned to the **Install Modules** page.

27.5 Updating the User and Admin Online Help

You can create an index of the online help files in Content Server, including help files that belong to Content Server modules. Indexing Content Server's online help enables users to perform full-text searches on help topics. For more information about Search Indexing, see *OpenText Content Server - Administering Search (LLESWBS-AGD)*.

Most Content Server modules contain associated help files for users and administrators. When you upgrade Content Server (or add, remove, or upgrade a module), the User and Admin Online Help indexes typically need to be updated. If the Help Data Source Folder or the Admin Help Data Source Folder indexes do not already exist, you must create them before you can update the help indexes.

> **Note:** Searching is one of the most common ways that users interact with online help. OpenText strongly recommends that you create indexes of both the admin and user online help to enable the Content Server help content to be searched.
>
> OpenText strongly recommends you delete and recreate the Help Data Source Folder and the Admin Help Data Source Folder whenever you add or remove language packs, or when the system default locale is modified.

27.5.1 To Update the Admin and User Online Help

To update the Admin and User Online Help:

1. In the **Search Administration** section of the Administration page, click **Open the System Object Volume**.

2. Update the User Help index:

   a. On the Content Server System page, click **Help Data Source Folder**..

   b. Click **Help Data Flow Manager**.

   c. In the **Processes** section of the **Help Data Flow Manager** page, click the **Functions** menu of the **Help Directory Walker**, and then click **Start**.

3. Update the Admin Help index

a. On the Content Server System page, click **Admin Help Data Source Folder**.
b. Click **Admin Help Data Flow Manager**.
c. In the **Processes** section of the **Admin Help Data Flow Manager** page, click the **Functions** menu of the **Admin Help Directory Walker**, and then click **Start**.

Note: OpenText strongly recommends you delete and recreate the Help Data Source Folder and the Admin Help Data Source Folder whenever you add or remove language packs, or when the system default locale is modified.

Part 7

User Setting Administration

Chapter 28

Administering Users and Groups

The topics in this section are written for the Content Server Administrator and for users who have the privilege to edit users and groups. Although some information may be duplicated, topics in the Administrator Help describe tasks from a system administrator's point of view. In many cases, only the Admin user or users with specific privileges can perform the tasks described in this section. For example, only the Admin user can view the Personal Workspace of a deleted user.

The Users and Groups Administration section allows you to configure user settings, such as passwords and name displays. You can also create and edit users and groups and configure department selections.

For general information about working with users and groups, see the user help topic *OpenText Content Server - Users and Groups (LLESWBU-UGD)*.

28.1 Configuring User Settings

When administering Content Server, you can specify the way in which Content Server displays the names of the users of your system. The display names can be configured individually for all languages that are enabled on the system.

You can preview each of the options in the **Example** field before finalizing your choice.

Setting User Password Restrictions

You can set password restrictions such as the minimum password length, a password expiration interval, and whether passwords must contain digits. To set the password restrictions for users you need to access the Directory Services user interface. For information about accessing the OTDS interface, see *OpenText Content Server - Administering OpenText Directory Services Integration Administration (LLESDSI-AGD)* and *OpenText Directory Services - Installation and Administration Guide (OTDS-IWC)*.

28.1.1 To Configure User Name Display

To configure the user name display:

1. Click the **Configure User Name Display** link in the **Users and Groups Administration** or **Languages** section of the Administration page.
2. On the Configure User Name Display page, choose the format you want displayed for each language from the **Display Name Format** list.
3. Select the **Append (Log-in ID) to Display Name** check box to have Content Server display the log-in ID in parentheses in addition to user names.
4. Click the **Submit** button.

28.2 Administering Users

When Content Server is first installed, there is only one user account, *Admin*, and one Department group, *DefaultGroup*. A Department group is the principal group of which a user is a member. Because each user in Content Server must belong to a department group, the Admin user is added to the DefaultGroup department group at install. After the installation and initial setup of Content Server is complete, you must create user accounts for each person that will be using Content Server, and organize those users into groups.

Once you have created users, you may grant another user the privilege to create or edit other users and groups of users.

Creating Users

In addition to the Admin user, any user with the *Can create/modify users* or *User administration rights* privilege can create a user. If you want to delegate the task of creating users to someone else, you must give that user the *Can create/modify users* or *User administration rights* privilege.

In some cases, the *Can create/modify users* privilege alone may not be sufficient when creating a new user. Every new user is assigned to a Department group in Content Server. A Department group is a user's home group. Users can be added to, or removed from, several other groups, but their Department typically does not change. Thus, if you have only the *Can create/modify users* privilege, you can create users in only those groups for which you are the creator or leader. To create a user anywhere in Content Server, you must also have the *Can create/modify groups* privilege or the *User administration rights* privilege.

If you are logged in as the Admin user for the purpose of creating users for the first time after installing Content Server, OpenText recommends that you create a set of empty Department groups first, so that those groups are available for selection as you create users.

It is important to note that a user with *User administration rights* privilege cannot grant system privileges to another that the creating user does not have. For example, if you do not have the *User administration rights* privilege, the **User Administration rights** check box does not appear.

After you assign passwords to new user accounts, advise the users to change the passwords as soon as they sign in to Content Server for the first time, and inform them of the password requirements.

For more information about creating, viewing, editing, or deleting users, see *OpenText Content Server - Users and Groups (LLESWBU-UGD)*.

For more information about setting user passwords, see "Configuring User Settings" on page 427 and *OpenText Directory Services - Installation and Administration Guide (OTDS-IWC)*.

Listing Users

When searching for users, Content Server displays no more than 30 users on a page by default. If your search criteria results in more than 30 users, the page contains a **More** button, which takes you to the next page of users. You can change this default by modifying the `MaxUsersToListPerPage` parameter in the`[general]` section of the *`<Content_Server_home>`*`/config/opentext.ini` file. Stop Content Server before you make changes to the `opentext.ini` file. When you are done, restart Content Server and, if applicable, the web application server so that your changes take effect.

You can also search for users without typing a search term. In this case, all entries for the specified field are displayed. However, on large Content Server systems with hundreds or thousands of users, such a broad search can adversely affect system performance.

28.2.1 To View the Personal Workspace of a Deleted User

To view the Personal Workspace of a deleted user:

Tip: You can access a deleted user's Personal Workspace from the Content Server Search page. Search for any item that resides in the deleted user's Personal Workspace. In the **Search Result** page's **Location** column, click the link of the Personal Workspace that you want to view.

1. Choose **Users & Groups** on the **Enterprise** menu.
2. On the **Users and Groups** page, bring up the Personal Workspace of an *existing* user. In the **Find** list, select the method you want to use for your search. Your choices are: User Last Name, User First Name, User Log-in, User E-mail.
3. In the **that starts with** dialog box, enter the first few letters of any *existing* user's name, log-in, or e-mail.
4. Click the **Find** button.
5. Click that existing user's **Browse** link in the **Actions** column. This will take you to that user's personal workspace.

6. In the browser's address bar, replace the ID at the end of the URL with the ID of the deleted user and press enter. The userid in the URL is displayed as **userID=<***number***>**.