Oracle® Fusion Middleware

Managing Oracle WebCenter Content

12c (12.2.1.4.0)
E95388-03
October 2021

Oracle Fusion Middleware Managing Oracle WebCenter Content, 12c (12.2.1.4.0)

E95388-03

Primary Author: Promila Chitkara

Contributors:

Contents

6 Managing Workflows

10 Managing Content Profiles

12 Managing a Records Retention Schedule

13 Managing Security for Records

14 Defining and Processing Dispositions

15 Managing the Oracle WebCenter Content Records Adapter

16 Managing Physical Content

18 Configuring Related Content (Links) for Records

19 Managing the Records System

22 Managing Inbound Refinery

23 Working with Conversions

24 Working With Image and Video Conversions

33 Managing Script Templates

43 Troubleshooting Inbound Refinery

Preface

This document describes common tasks used to manage Oracle WebCenter Content applications, including content management, workflows, content retention and record management, and imaging management.

Audience

This document is intended for use by Oracle WebCenter Content application administrators who manage a subset of system administration tasks.

Documentation Accessibility

For information about Oracle's commitment to accessibility, visit the Oracle Accessibility Program website at http://www.oracle.com/pls/topic/lookup?ctx=acc&id=docacc.

Access to Oracle Support

Oracle customers that have purchased support have access to electronic support through My Oracle Support. For information, visit http://www.oracle.com/pls/topic/lookup?ctx=acc&id=info or visit http://www.oracle.com/pls/topic/lookup?ctx=acc&id=trs if you are hearing impaired.

Related Documents

The complete Oracle WebCenter Content documentation set is available from the Oracle Help Center at http://www.oracle.com/pls/topic/lookup?ctx=fmw122140&id=wcc-books.

Conventions

The following text conventions are used in this document.

Convention	Meaning
boldface	Boldface type indicates graphical user interface elements associated with an action, or terms defined in text or the glossary.
italic	Italic type indicates book titles, emphasis, or placeholder variables for which you supply particular values.
`monospace`	Monospace type indicates commands within a paragraph, URLs, code in examples, text that appears on the screen, or text that you enter.

Oracle WebCenter Content Terminology

Oracle WebCenter Content documentation uses the following terms when referring to variables in the directories associated with the Oracle WebCenter Content and Oracle WebCenter Content Server configuration:

- *IdcHomeDir*: This variable refers to the `ucm/idc` directory in the Oracle WebCenter Content home where the Oracle WebCenter Content server media is located. The server media can run Oracle WebCenter Content Server, Oracle WebCenter Content: Inbound Refinery, or Oracle WebCenter Content: Records software. This is essentially a read-only directory. The default location is *`WCC_ORACLE_HOME`*`/ucm/idc`. The variable portion of the default location can be changed, but the path cannot be changed from `ucm/idc`.
- *DomainHome*: This variable refers to the user-specified directory where an Oracle WebCenter Content application is deployed to run on an Oracle WebLogic Server application server. The *`DomainHome`*`/ucm/`*`short-product-id`*`/bin` directory contains the `intradoc.cfg` file and executables. The default location for *`DomainHome`* is *`MW_HOME`*`/user_projects/domains/`*`base_domain`*, but you can change the path and domain name (*`base_domain`*) during the deployment of an Oracle WebCenter Content application to an application server.
- *short-product-id*: This variable refers to the type of Oracle WebCenter Content server deployed to an application server. This name is used as the context root (default `HttpRelativeWebRoot` configuration value). Possible values include:
  - `cs` (Oracle WebCenter Content Server)
  - `ibr` (Oracle WebCenter Content: Inbound Refinery)
  - `urm` (Oracle WebCenter Content: Records
- *IntradocDir*: This variable refers to the root directory for configuration and data files specific to an Oracle WebCenter Content instance that is part of an Oracle WebCenter Content application deployed to an application server. This Idoc Script variable is configured for one type of Oracle WebCenter Content instance: Content Server (`cs`), Inbound Refinery (`ibr`), or Records (`urm`). This directory can be located elsewhere, but the default location is *`DomainHome`*`/ucm/`*`short-product-id`*. The specified directory must be an absolute path to the instance directory and must be unique to a particular server or node. The directory includes a `bin/` directory, which contains the startup files (`intradoc.cfg` and executables).

Part I
Understanding Oracle WebCenter Content

This section provides an overview of the applications included in Oracle WebCenter Content. It also discusses common tasks undertaken by an administrator when managing Oracle WebCenter Content applications.

Understanding Oracle WebCenter Content contains the following chapter:

- Introduction to Oracle WebCenter Content Features

1

Introduction to Oracle WebCenter Content Features

Oracle WebCenter Content provides a number of features for configuring and managing content in the repository, including functionality such as organizing content into folders and folios, using workflows, managing different types of content, converting content from and to different formats, and using retention schedules to manage the life cycle of content.
This chapter discusses the following WebCenter Content features and provides a roadmap of basic tasks for managing the functionality.

1.1 Content Management

The content repository is the heart of Oracle WebCenter Content. All content checked in to the system is stored in the repository and from there it can be managed by users with the appropriate permissions for that content.

By using Oracle WebCenter Content, an organization can utilize a unified repository to house unstructured content, and deliver it to business users in the proper format, and within the context of familiar applications to fit the way they work.

Content Server

Content Server is the foundation for a variety of Oracle content management applications. It provides a flexible, secure, centralized, web-based repository that manages all phases of the content life cycle from creation and approval to publishing, searching, expiration, and archiving or disposition.

Every contributor throughout the organization can easily contribute content from native desktop applications, efficiently manage business content via rich library services, and securely access that content anywhere using a web browser or mobile app. Contributors have several ways to interact with content:

- Web browser

- Mobile apps
- Desktop client

For information about working with content using a web browser or mobile apps, see *Oracle Fusion Middleware Using Oracle WebCenter Content*. For information about using the desktop client, see *Oracle Fusion Middleware Using Oracle WebCenter Content: Desktop*.

Content Repository

All content, regardless of content type, is stored in the web repository or database for management, reuse and access. While stored in the repository, all types of content – ranging from email, discussions, documents, reports, spreadsheets and records to images, multimedia or other digital formats – receive the same set of fundamental core services.

Components

A number of components providing advanced functionality are included with Content Server. These components may be rolled into the core or available to be enabled after installation.

For more information on managing content, see Managing Content .

1.2 Folders

Folders, a scalable and enterprise solution, implemented with the FrameworkFolders component, provides a hierarchical folder interface similar to a conventional file system for organizing and locating some or all of the content in the repository.

Query folders can be used to return content based on a query associated with the folder. These types of folders can also have retention dispositions associated with the folder.

For more information on folders, see Organizing Content.

1.3 Folios

When enabled, Content Folios provides a quick and effective way to assemble, track, and access logical groupings of multiple content items from within the secure environment of Content Server. For example, all items relevant to an upcoming brochure, such as images, logos, legal disclosures, and ad copy, can be assembled and sent through a workflow process. Once approved, all associated content can be downloaded and sent for print.

Or perhaps a new project requires a virtual place to assemble all relevant content items in a particular hierarchy, whenever they are checked in, with restricted access to particular areas of the hierarchy. Or a video may need to be associated and tracked with release waivers and narration text. All this can be done with Content Folios.

Technically, a content folio is an XML file checked into the repository that uses elements to define a hierarchical structure of nodes, slots, and specified content items in Content Server. In practice, a content folio is a logical grouping, or a framework in which content stored in the repository can be structured. Simple folios are a flat container, while advanced folios can nest content in a hierarchy within folders. In an

advanced folio, the hierarchy may be established prior to assembling content items, or it may be created during or subsequent to assembling the items.

Existing folios can have content added to them, or can be locked so that no changes can be made. Content items can be added to a simple folio by searching Content Server, and to an advanced folio by checking new items into the repository or by searching for content that has previously been checked in, all through the folio interface. An advanced folio can even contain links to outside resources such as websites or shared network drives.

For more information on folios, see Organizing Content.

1.4 Workflows

Workflows are used to specify how content is routed for review, approval, and release to the system. This chapter provides an overview, tasks, and reference information for using the workflow functionality available with Oracle WebCenter Content Server.

Setting up workflows for a business process can provide several advantages:

- Workflows provide good reporting metrics. They can produce an audit trail of who signed off on content at various points of the life cycle of the content.
- Workflows help get the right information to the right person.
- Designing a workflow requires you to examine and understand your business processes, helping you find areas for improvement.

For more information, see Managing Workflows.

1.5 Digital Asset Manager

Digital Asset Manager (DAM) is used to define and provide images and videos in specified formats and sizes for download by the people in your organization who need them. This helps your organization maintain consistent standards for branding and digital content use.

DAM creates multiple formats of digital assets automatically when an image or video is checked into Content Server and lists the formats under one content ID. This ensures that the asset, such as a corporate logo or promotional video, maintains a standard size and quality in the multiple formats required by your organization, while providing the content management and workflow applications of Content Server. For example, one person can download images of the logo for use on a web-site, and another can download and bundle images of the same logo for use in office presentations or print collateral, all from a single digital asset checked into the repository.

Digital assets are valuable electronic images and videos to be made available within your organization in multiple output formats, called *renditions*. The quantity and type of renditions are defined by the system administrator in rendition sets. A user selects a rendition set to create renditions of a digital asset at the time the asset is checked into the repository.

For more information, see Working With Image and Video Conversions.

1.6 Records

Using the Oracle WebCenter Content: Records functionality, content items can be managed on a retention schedule, which determines the life cycle of each content item. The focus of *records management* tends to be the preservation of content for historical, legal, or archival purposes while also performing retention management functions. The focus of *retention*

management tends to be the scheduled elimination of content in which the costs of retaining content outweighs the value of keeping it. The Records functionality combines both record and retention management into one software system. You can use this functionality to track and to preserve content as needed, or to dispose of content when it is no longer required.

Different reasons may exist for why organizations need to retain content. Many organizations are subject to regulations that require the retention of information for a specified period, such as compliance with Sarbanes-Oxley regulations, government regulations such as DoD 5015.2. An organization may have a litigation-related need for effective and efficient retention management. Or an organization may want to provide a uniform infrastructure for retrieving and sharing content. The Records options can be configured and customized to fit any of these business needs.

In addition to internal content (electronic items stored within Content Server), the Records application can manage external content. An ***external*** retained content item can be in a variety of formats, both physical or electronic. If the source file is not specifically stored in Content Server, then it is considered external. The software can manage the disposition schedule, search metadata associated with the external file, and manage an electronic rendition of an external file. An electronic rendition can either be checked in as a primary file of an external item, or be filed as a separate file, and then linked to the external file metadata.

The Records application can be used to manage classified content which requires protection against unauthorized disclosure (for example, because it contains information sensitive to the national security of the United States or because it is essential for a corporation's operation). Options can be chosen during configuration to ensure that the system complies with the DoD 5015.2 standard (including Chapter 4). The software has been certified by the Joint Interoperability Test Command (JITC) to comply with that standard.

For more information, see Managing Records.

1.7 Content Conversion

Several different conversion applications are available to publish native content items in different formats as needed at your site. The following conversion applications are discussed in this section:

- Inbound Refinery
- Other Conversion Formats
- PDF Watermark

For more information, see Managing Content Conversion.

1.7.1 Inbound Refinery

Basic thumbnail creation is automatically supplied for supported content file types in Content Server. However, you can use Inbound Refinery to manage all file conversions at the input side of Content Server. Inbound Refinery also provides the ability to convert native content items to web-viewable PDF (Portable Document Format) files. Files are converted on check-in of the content into Content Server.

Inbound Refinery includes Outside In Image Export, which can be used for the following:

- To create thumbnails of files checked into the repository. Thumbnails are small preview images of content. Outside In Image Export can also be used to create thumbnails of PDF files generated by Inbound Refinery.
- To convert files checked into the repository to multi-page TIFF files as the primary web-viewable rendition.

Inbound Refinery includes the PDFExportConverter component (installed but disabled by default on WebCenter Content). PDFExportConverter uses Outside/In libraries for cross-platform conversion of files to PDF.

In addition to the conversions that Inbound Refinery can perform using Outside In Image Export, several conversion components are available for use with Inbound Refinery. The additional types of files that Inbound Refinery can convert, and the result of each conversion, depend on the conversion components that are enabled on the Inbound Refinery instance.

The WinNativeConverter component enables Inbound Refinery to automatically publish native content items to web-viewable PDF (Portable Document Format) files. A PDF rendition of the native format is immediately generated upon check-in of new content into the repository. This PDF rendition allows web viewing of that content item without requiring users to install native applications. Over 35 file formats can be converted to PDF, such as Adobe Framemaker, Illustrator, InDesign, PageMaker, and Photoshop as well as Hangul, JustSystems Ichitaro, Lotus Smartsuite, Microsoft Office, and Microsoft Visio. For more information about supported formats, see Supported File Formats.

Inbound Refinery also can optimize non-optimized PDF files and process links such as Microsoft Word links, 'mailto' links, and table-of-content links.

1.7.2 Other Conversion Formats

XML Converter gives XML-based access to information in unstructured business content. With XML Converter, content contributed to Content Server is converted to XML at the time of check-in. XML Converter converts over 225 document types and supports the leading word processing formats, such as Microsoft Word, Lotus WordPro, and Corel WordPerfect. It also includes support for popular spreadsheet, presentation, and graphic formats.

When a new content item is checked into the repository, XML Converter converts the content to either a SearchML or FlexionDoc format. FlexionDoc is verbose and captures extensive information, including attributes such as styles in a Microsoft Word document. From there, administrators have the ability to check in different XSL files that would then convert the SearchML or FlexionDoc document to any XML format.

Tiff Converter enables organizations to check TIFF (Tagged Image File Format) files into Content Server and then publish these as multiple-page PDF files. Tiff Converter uses either CVISION CVista PdfCompressor or Adobe Acrobat Capture to convert single-page TIFF files, multiple-page TIFF files, or zip files containing multiple TIFF files (TIFZ, TIZ or ZIP file extensions) to a single PDF file. Additionally, during the TIFF to PDF conversion, Optical Character Recognition (OCR) is performed, enabling users to perform full-text searches of managed TIFF files in Content Server.

1.7.3 PDF Watermark

PDF Watermark allows watermarks to be applied to PDF files generated by PDF Converter (static watermarking) and returned to the repository. Existing PDF files in the repository can also be watermarked (dynamic watermarking). Dynamic watermarks are generated as needed and can contain variable information (for example, user name, date and time of

download, or file name). System administrators can define variables and set up specific conditions for generating dynamic watermarks.

PDF Watermark can also add security features to PDF files as they are downloaded for viewing. Access settings can be enabled or disabled, such as printing or modifying the file.

1.8 Dynamic Converter

Dynamic Converter is a transformation technology and on-demand publishing solution for critical business documents. With Dynamic Converter, you can easily convert any business document into a Web page for a specified audience without use of the application used to create that document. The benefits are immediate. Information can be exchanged freely without the bottleneck of proprietary applications.

When a Web browser first requests a document, a set of rules is applied to determine how that document should appear as a Web page. These rules can be defined in a template, a core component of Dynamic Converter.

Dynamic Converter offers a number of benefits to the user:

- Business documents can be easily viewed in a Web browser.
- Native applications (such as Adobe Acrobat, Microsoft Word, and so on) are not required.
- Multiple renditions of a document are available for different devices (Web browsers, wireless devices, and so on).
- Numerous business document types, including legacy formats, are supported.

For more information, see Managing Dynamic Conversion.

1.9 Desktop

The Desktop application provides a set of embedded applications that help you seamlessly integrate your desktop experience with Content Server. More specifically, it provides convenient access to the repository from Microsoft Windows Explorer, desktop applications like Microsoft Word and Excel, and email clients like Microsoft Outlook and Lotus Notes.

As a result, you can easily manage files in the repository and share files with users directly from your desktop instead of logging into Content Server and using a web browser.

For more information, see Managing Desktop.

1.10 Basic Tasks for Configuring and Managing Oracle WebCenter Content Applications

The roadmap in Table 1-1 outlines tasks that the WebCenter Content administrator can perform to manage WebCenter Content applications after WebCenter Content has been installed and the system configured. These tasks are in addition to system management tasks, which are documented in *Administering Oracle WebCenter Content*. The WebCenter Content administrator can perform both system-level and

application-level tasks, or one or more additional WebCenter Content administrators can be created to perform just the applications tasks.

Table 1-1 Roadmap for Basic Management Tasks

Task	Description and Documentation Links
Get started using WebCenter Content	Access WebCenter Content, start and stop the servers, and monitor server status: • Getting Started Managing Oracle WebCenter Content • Finding Status and Error Information
Configure content	Configure content display, content metadata, email, electronic signatures, content types, and profiles: • Starting the Repository Manager • Configuring the Repository Manager Content List • Managing Content Using Repository Manager • Managing Revisions Using Repository Manager • Subscribing to Content • Signing Content Electronically • Defining Content Types • Customizing Repository Fields and Metadata • Categorizing and Linking Content • Managing Content Profiles
Manage content	Organize content into hierarchies and groupings, and monitor access to content: • Managing Folders • Managing WebDAV • Managing Content Folios • Managing Desktop • Tracking Content Access
Manage workflows	Create workflows, which are used to specify how content is routed for review, approval, and release to the system: • Creating a Criteria Workflow • Creating a Basic Workflow • Customizing Workflows

Table 1-1 (Cont.) Roadmap for Basic Management Tasks

Task	Description and Documentation Links
Convert content into different formats	Set conversion configuration options and file formats: • Configuring Inbound Refinery Configure refinery user authentication, monitor performance, publish layout files: • Managing Refinery Authentication and Users • Managing Refinery Conversion Queues • Publishing Dynamic and Static Layout Files • Changing the Date Format and Time Zones • Monitoring Refinery Status Convert native files to other formats: • Managing PDF Conversions • Managing Tiff Conversions • Managing XML Conversions • Converting Microsoft Office Files to HTML Work with converted content: • Viewing Content Information • Viewing a Converted File • Previewing a Document Before Check-In Define images, videos, and audio files in specified formats and sizes for download: • Configuring Digital Asset Manager • Setting Up and Managing Image Conversions • Setting Up and Managing Video Conversions Apply a watermark at check-in or during viewing of PDF: • Configuring PDF Watermark
Perform on-demand document conversion	Configure the Dynamic Converter default template, conversion formats, slideshow template files, and remove wireless templates: • Configuring Dynamic Converter Configure sets of instructions that drive the conversion process: • Managing Template Rules Choose and implement templates that drive the conversion process and provide control over the visual and navigational properties of the converted web page: • Managing Conversion Templates Use HTML Conversion templates, script templates, and snippits: • Using the HTML Conversion Template Editor • Creating a Layout Template for Your Content Items • Setting Script Template Formatting Options View information on converted content, view converted content, and preview HTML renditions: • Viewing Content Information • Viewing a Converted File • Previewing a Document Before Check-In

Table 1-1 (Cont.) Roadmap for Basic Management Tasks

Task	Description and Documentation Links
Manage content items on a retention schedule (optional)	Plan how to use Oracle WebCenter Content: Records with a content retention schedule, how to manage physical content, and how to set up workflows to manage reservation and off-site processing: • Configuring Records Management Set up a retention schedule and objects in the schedule, manage a series, manage a retention category, and manage a retention folder: • Managing a Records Retention Schedule Manage records security including retention management roles, permissions, custom security fields, Access Control Lists, and supplemental markings which are required for compliance with the DoD 5015.2 specification: • Managing Security for Records Manage dispositions (actions) on content, using triggers and freezes: • Defining and Processing Dispositions Manage the Content Server adapter which provides a bridge between the record system and the Content Server repository: • Managing the Oracle WebCenter Content Records Adapter Manage physical records and content that are not stored in the repository in electronic form: • Managing Physical Content • Processing Reservations and Chargebacks Schedule tasks for completion, create reports, create custom scripts, and monitor activity: • Configuring Related Content (Links) for Records • Managing the Records System Manage federated searches and freezes: • Using Federated Search and Freeze

For details about installing WebCenter Content, see *Installing and Configuring Oracle WebCenter Content*.

Part II
Basic Applications Administration

This part provides information on the administrative responsibilities and tools used to manage different Oracle WebCenter Content applications.

Basic Applications Administration contains the following chapters:

- Getting Started Managing Oracle WebCenter Content
- Finding Status and Error Information

2

Getting Started Managing Oracle WebCenter Content

This chapter provides an overview of administrative responsibilities and tools used to manage different Oracle WebCenter Content applications. It also provides an overview of the interface to help guide the administrator when managing these applications.
This chapter contains the following topics:

2.1 Understanding Management Responsibilities

Oracle WebCenter Content administrators are responsible for configuration and performance management of the WebCenter Content system.

WebCenter Content administrators also configure and manage WebCenter Content applications to control storage and use of content in the repository. A WebCenter Content administrator can be assigned to work specifically with one or more of these applications, which are documented in this guide. Management tasks can include the following:

- Populate the site with content
- Manage conversion of content into different formats
- Create and maintain user profiles
- Create and maintain workflows which direct content to users for specified actions
- Create custom metadata to be associated with content
- Perform Records Administrator duties (create and manage content retention schedules, process dispositions, and so forth)
- Perform administrative duties as directed

To see a roadmap showing basic management tasks and links to specific information in this guide, see Basic Tasks for Configuring and Managing Oracle WebCenter Content Applications.

2.2 Understanding Management Tools

The following Content Server tools can be started as standalone applications from the Admin Applets page (see Figure 2-2), as applets through a web browser, or by choosing the **Apps** menu in each of the tools.

- **Configuration Manager**: Manage content types, file formats, and custom metadata fields.
- **Repository Manager:** Perform file diagnostics, file management functions, search data re-indexing, and subscription management functions.
- **Weblayout Editor:** Build a Website, work with reports, write queries.
- **Workflow Admin**: Set up workflows to route content to specific people for action.

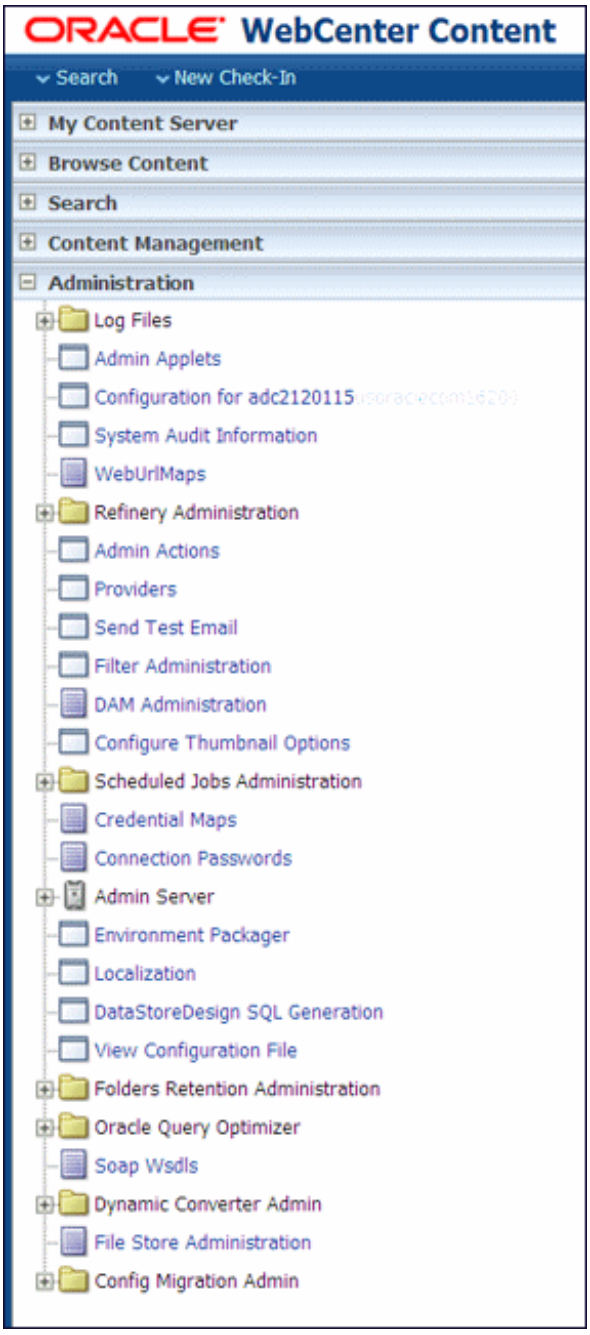
Other Oracle WebCenter Content applications, such as Oracle WebCenter Content: Inbound Refinery and Oracle WebCenter Content: Records, are installed separately and can be accessed through the Administration tray or menu on the Oracle WebCenter Content interface home page.

2.3 Interface Overview

The Administration tray is the default layout in the Content Server interface to provide access to pages for configuring and managing Oracle WebCenter Content applications.

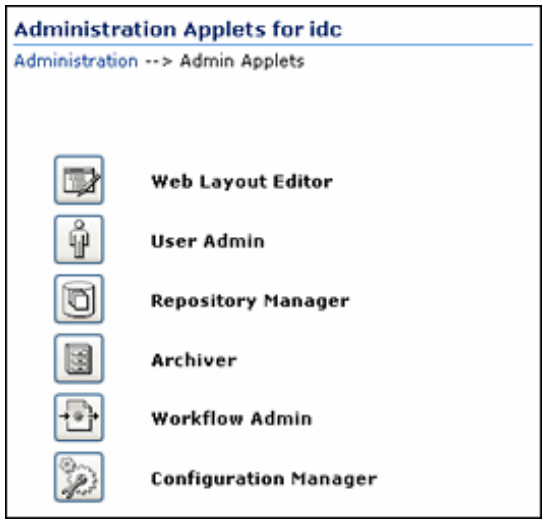
To access the Administration tray, log in as a Content Server administrator, then choose **Administration** in the home page to view available administration options. If your Content Server instance is configured to use the Menus layout, choose **Administration** to view the same options. Figure 2-1 shows a sample Oracle WebCenter Content tray layout with the Administration selection expanded to show options.

Figure 2-1 Sample Oracle WebCenter Content Administration Tray



To access administration applications, choose **Administration**, then choose **Admin Applets**. The Admin Applets page displays with links to Oracle WebCenter Content applications.

Figure 2-2 Admin Applets Page



If installed with Oracle WebCenter Content, applications such as Inbound Refinery or Records Management can be accessed from the **Administration** selection. See Figure 2-1.

> **Note:**
>
> Administrators use the *native interface* to perform administrative tasks and access software utilities in WebCenter Content. The WebCenter Content application is configured by default to use the native interface for both administrators and users. If WebCenter Content is configured to use the *WebCenter Content user interface* (new as of 11.1.1.8), administrators must still use the native interface.
>
> For more information on the WebCenter Content user interface, see Getting Started with the WebCenter Content User Interface in *Using Oracle WebCenter Content*.

2.4 Starting and Stopping Oracle WebCenter Content Server and Inbound Refinery Instances

There are several methods for starting and stopping a WebCenter Content Server instance. Which method you choose depends on your requirements, your authorization, and the task you want to complete. For example, when certain configuration changes are made to a Content Server instance, such as when components are enabled or disabled, the instance must be restarted.For the Inbound Refinery (IBR) instance, the only method available is to use Oracle Enterprise Manager Fusion Middleware Control.

For details on how to use these methods, see Starting and Stopping Content Server and Inbound Refinery in *Administering Oracle WebCenter Content*.

2.5 Accessing Oracle WebCenter Content Instances

To access a running WebCenter Content instance as an administrator, start a web browser and enter the URL for the specific WebCenter Content instance type: Content Server, Inbound Refinery, Imaging, or Records. For details on how to access each type of instance, see Accessing Oracle WebCenter Content Instances Using a Web Browser in *Administering Oracle WebCenter Content*.

2.6 Running Administration Applications as Applets

You can run several of the Content Server administration applications as applets from any browser with access to the Content Server instance. Applets are convenient for remote administration.

The Batch Loader, Component Wizard, System Properties, and Content Server Analyzer utilities cannot be run as applets; for security reasons, they must be run in standalone mode from the computer where the Content Server instance is installed. See Running Administration Applications in Standalone Mode.

Some functions that are available in the standalone version of an application are not available from the applet version. See the documentation for each application for more information.

To run an administration application as a Java applet within a Java-enabled browser:

1. Open a browser window.
2. Log in to the Content Server instance as an administrator or subadministrator.
3. Choose **Administration** then choose **Admin Applets**.

2.7 Running Administration Applications via the Oracle WebCenter Content Administration App

You can run these Content Server administration applications using the desktop admin app: Archiver, Configuration Manager, Content Categorizer Administration, Data Engine Control Center, PDF Watermark Administration, Repository Manager, User Admin, Web Layout Editor, and Workflow Admin. You can also run the admin app in a browser via the native user interface.

The Batch Loader, Component Wizard, System Properties, and Content Server Analyzer utilities cannot be accessed via the desktop app for security reasons. They must be run in the standalone mode from the computer where the Content Server instance is installed. See Running Administration Applications in Standalone Mode.

Some functions that are available in the standalone version of an application are not available in the desktop app. See the documentation for each application for more information.

Before You Begin

- The desktop admin app is supported only for 12.2.1.4.0 and higher releases.
- The desktop admin app supports the corporate single sign on (SSO).
- In the scenarios where the Content Server is front-ended by a load balancer or Oracle HTTP Server, the desktop admin app uses the URL of either of these to access the Content Server.

- The desktop admin app is designed to run on Windows, Mac, and Linux. See the certification matrix for information on the supported versions of these operating systems.
- If you have not already installed the admin app, you can do so now. Installers for Windows, Mac, and Linux are available for download via **Content Server Home** > **Administration** > **Admin Applets**. The URL should look like this: `http://example.com:16200/cs/idcplg?IdcService=GET_ADMIN_PAGE&Action=GetTemplatePage&Page=ADMIN_APPLETS`

> **Note:**
>
> After the installation is successfully completed, a desktop icon is created for you.
> The desktop admin app is installed at the following locations:
>
> - **Windows**: `C:\Program Files\Oracle WebCenter Content Administration`. If the `c:\` drive is not available, the installer automatically detects the program files folder, and the app is installed in that folder. To set proxy, if you use a server URL and port instead of a `pac` script, ensure that the URL is configured in the Internet Explorer options.
> - **Mac**: `/Applications/Oracle WebCenter Content Administration`On Mac, the proxy should be configured in **Safari** > **Preferences**.
> - **Linux**: Where `.tar` is extracted. On Unix, you can set the proxy server in the terminal before launching the script: `export http_proxy=http://my.proxyserver.net:8080/`

- Once you've downloaded the `.tar` file for Linux, untar it. Instructions to install the admin app on Linux are available in the `README` file located in the `wccadmin` folder.
- When a new version of the admin app is available, the following message is displayed on your screen when you try to launch an older version of the app:

  This version of the Administration client is too old to connect to the Content Server. Please install the Administration client associated with the Content Server.

On Windows and Mac, you can launch the app from the browser via the CS Admin Applets page by clicking **Launch Client**. To use the desktop admin app in a browser, you must first specify the Http server address in the `config.cfg` of the Content Server, if it's not already specified.

To run an administration application using the desktop app:

1. Double-click the desktop icon that is created after you install the app.
2. In the **Oracle WebCenter Content - Administration** dialog, log in to the Content Server instance as an administrator or subadministrator:
   a. In the **User Name** field, enter the user name that has access rights.
   b. In the **Password** field, enter the password.
   c. In the **Server** field, enter the server address of your Content Server instance in this format: `https://host.example.com:16200/cs/`

If the Content Server version is compatible with the desktop admin app, then the app connects to the server and the last connected server URL is saved in this field. You can select the this URL from this drop-down list for subsequent logins. In case you try to connect to incompatible versions, an error message is displayed.

d. Click **OK**.
The WebCenter Administration app is displayed. This app lets you configure and manage the following applications: Archiver, Configuration Manager, Content Categorizer Administration, Data Engine Control Center, PDF Watermark Administration, Repository Manager, User Admin, Web Layout Editor, and Workflow Admin.

> **Note:**
>
> The application are listed based on the users privileges and the components that are enabled in the Content Server.

3. In the WebCenter Administration app, click the application you want to configure or whose configurations you want to edit to display its configuration page.

2.8 Running Administration Applications in Standalone Mode

You can run all Content Server administration applications in standalone mode from the computer where the Content Server instance is installed. The method required to start these programs differs slightly between Windows and UNIX installations. Running the standalone version of an application offers greater security than browser applets, and enables you to send passwords without having them captured or copied from the web or a network.

Standalone administration applications require that the Content Server system administrator running the applications be a *local* admin user, instead of a user defined through Oracle WebLogic Server. (Local users are otherwise unused in Oracle WebLogic Server.) To use standalone administration applications that require a login, run the User Admin applet and define a new local user with Admin permissions in Content Server.

> **Important:**
>
> Before you can run Content Server administration applications in standalone mode, additional configuration is required to authenticate the applications on Oracle WebLogic Server and to establish a JDBC connection to the system database and access to the Oracle WebLogic Server database connection.

For more information, see the following topics in *Administering Oracle WebCenter Content*:

- Local Users
- Adding a User Login
- Configuring a JDBC Database Driver for Standalone Mode

2.8.1 Standalone Administration Applications on Windows Systems

To run a standalone administration application on a Windows operating system:

1. From the Windows Start menu, select the application:
   - To run one of the configuration applications, choose **Start**, then **Programs**, then **Content Server**, then ***instance***, then ***application***.
   - To run one of the administration utilities, choose **Start**, then **Programs**, then **Content Server**, then ***instance***, then **Utilities**, then ***utility***.

   For all applications except for Component Wizard and System Properties, a login window opens. For Component Wizard and System Properties, the main window of the application opens.

   > **Tip:**
   >
   > It may take several seconds for the login window or the application window to appear, and the window may be hidden by other windows.

2. Enter the administrator login name and password.
3. Click **OK**.

   The main screen of the application opens.

2.8.2 Standalone Administration Applications On UNIX Systems

To run a standalone administration application on a UNIX operating system:

1. Navigate to the *DomainHome*`/ucm/cs/bin/` directory.
2. Executable applications are listed. Enter ***`./application_name`***, where *`application_name`* is the name of one of the executable files. If an application is not listed, it can be entered as a parameter to the IntradocApp application, as in this example:

   ```
   % ./IntradocApp Workflow
   ```

3. Press **Enter**. For all applications except for Component Wizard and System Properties, a login window opens. For Component Wizard and System Properties, the main window of the application opens.
4. Enter the administrator login name and password.
5. Click **OK**.

   The main window of the application opens.

3
Finding Status and Error Information

This chapter provides information on sources of Oracle WebCenter Content information that can be helpful in the troubleshooting process.

3.1 Monitoring Content Server Status

Information on several Content Server internal resources that are useful in monitoring the status of a Content Server instance is available in *Administering Oracle WebCenter Content*. These resources include:

- Content Server status
- Java output
- System configuration information
- System audit information
- Scheduled jobs

3.2 Monitoring Content Server Logs

Information on finding and using Content Server status information and errors in log files is available in *Administering Oracle WebCenter Content*. This information includes:

- Log file characteristics
- Accessing Content Server logs
- Accessing Archiver logs
- Accessing Inbound Refinery logs

Part III
Managing Content

This section of the documentation discusses managing repository content using Oracle WebCenter Content.

Managing Content contains the following chapters:

- Managing Content
- Organizing Content
- Managing Workflows
- Customizing Repository Fields and Metadata
- Categorizing and Linking Content
- Tracking Content Access
- Managing Content Profiles

4
Managing Content

This chapter discusses how to manage content items, revisions, subscriptions and the Indexer, using the Repository Manager application.
This chapter discusses the following topics:

- Starting the Repository Manager
- Configuring the Repository Manager Content List
- Managing Content Using Repository Manager
- Managing Revisions Using Repository Manager
- Subscribing to Content
- Signing Content Electronically
- Managing Native Content Conversion
- Defining Content Types

4.1 Starting the Repository Manager

The Repository Manager can be run as an applet or in standalone mode.

To run the Repository Manager as an applet:

1. Use the main menu to choose **Administration**, then **Admin Applets**.
2. Choose **Repository Manager**.

   The Repository Manager applet opens.

To run Repository Manager in standalone mode, see the instructions in *Administering Oracle WebCenter Content*.

Use the **Functions** menu of the Repository Manager to perform a variety of administrative functions on specific revisions. Right-click a revision when displaying the revisions with the filter to open a shortcut menu, which includes all of the options on the **Functions** menu.

4.2 Configuring the Repository Manager Content List

Administrators and subadministrators with RepMan rights can display a list of content item revisions in the Repository Manager. Administrators can display all content items; subadministrators with RepMan rights can display only content items for which they have Admin permission to the security group and account (if applicable). Search the revision list by specifying metadata fields and revision status as filter criteria.

This section discusses the following topics:

- Changing Column and Filter Settings
- Changing Default Sort Order

4.2.1 Changing Column and Filter Settings

To filter the Content list by revision:

1. On the **Content** tab of the Repository Manager application, select the **Use Filter** check box, then click **Define Filter**.
2. On the Define Filter page, select the check boxes for the filter criteria to use and add values for the fields.
3. Click **OK**.

To filter revisions by Release Date:

1. On the **Content** tab of the Repository Manager application, select **Release Date Since**.
2. Select a predefined date range.
3. Click **OK**.

To change the columns displayed on the **Content** tab:

1. On the **Content** tab of the Repository Manager application, click **Show Columns**.
2. On the Show Columns page, select the columns to be displayed. Custom fields are at the bottom of the list.
3. Click **OK**.

4.2.2 Changing Default Sort Order

When the Repository Manager application is started, it runs a default query against the database that returns all content released the previous day. By default, the query sorts the results by the ContentID of the content items.

Ordering by ContentID is advantageous because the order is predictable when the Repository Manager has a long list of content items. But sorting by ContentID can be time-consuming. It may be preferable to have faster query results without the predictable order.

To change the order, disable the `DoDocNameOrder` configuration setting. When the value is set to true (the default), content items are sorted by ContentID. When set to false, content items are not sorted. When the sort order is changed to optimize the query, enable the JDBC Query Trace to log trace information to the console log where database queries can be viewed.

4.2.2.1 Disabling the `DoDocNameOrder` configuration setting:

To disable the `DoDocNameOrder` configuration setting:

1. In a text editor, open the *`IntradocDir`*`/config/config.cfg` file.
2. Add the following configuration setting:

   ```
   DoDocNameOrder=false
   ```

3. Save and close the `config.cfg` file.
4. Restart Content Server.

4.2.2.2 Enabling query tracing

To enable Query Tracing:

1. Use the main menu to choose **Administration** then **System Audit Information**.
2. On the System Audit Information page, scroll to the bottom of the **Edit Active Console Output Tracing** section.
3. From the **Action Sections** list, select **systemdatabase**.

   The `systemdatabase` is added to the list of active sections.
4. Click **Update**.
5. Restart Content Server.

For more information about tracing reports and restarting Content Server, see *Administering Oracle WebCenter Content*.

4.3 Managing Content Using Repository Manager

Several common tasks are done when managing content and revisions with Repository Manager, as discussed in the following sections:

- Adding a New Content Item
- Managing Content Metadata
- Managing Expired Content

4.3.1 Adding a New Content Item

To add a new content item using the Repository Manager:

> **Note:**
>
> New content items cannot be added using the Repository Manager launched as a Java applet from a browser. Use the standalone application. For details on using standalone applications, see *Administering Oracle WebCenter Content*.

1. Start the Repository Manager in standalone mode.
2. Click the **Content** tab.
3. Click **Add New**.
4. On the Add New Content Item page, enter the required and optional information for the content item.
5. Click **OK**.

   The specified file is checked in as a new content item.

4.3.2 Managing Content Metadata

This section provides information on how to view or update the metadata fora revision using the Repository Manager.

4.3.2.1 Viewing the metadata for a revision

To view the metadata for a revision using the Repository Manager:

1. Use the main menu to choose **Administration** then **Admin Applets**.
2. Choose **Repository Manager** then the **Content** tab.
3. Highlight the revision for metadata review.
4. Choose **Functions** then **Info** or right-click and click **Info**.
5. On the Approve Revision page, click **OK** to close the page.

4.3.2.2 Updating the metadata for a revision

To update the metadata for a revision using the Repository Manager:

1. Use the main menu and choose **Administration** then **Admin Applets**.
2. Choose **Repository Manager** then the **Content** tab.
3. Select the revision to update.
4. Choose **Functions**, **Update**, or right-click and select **Update**.
5. On the Update Content Info page, enter new metadata as necessary.
6. Click **OK**.

   The metadata is updated without checking in a new revision.

4.3.3 Managing Expired Content

This section describes how to manage expired content.

4.3.3.1 Reviewing expired content from Repository Manager

To review expired content from Repository Manager:

1. Use the main menu to choose **Administration** then **Admin Applets**.
2. Choose **Repository Manager** then the **Content** tab.
3. From the **Content** tab, select **Define Filter**.
4. On the Define Subscription Filter page, select **Enable Revision Status**, and select **Expired**.

   A list of expired content is displayed.

4.3.3.2 Automating email notification for expired content

To automate email notification for the author and administrator when the content expires:

1. Edit *IntradocDir*`/config/config.cfg` in a text editor and enter the following:

   ```
   EnableExpirationNotifier=1
   ```

2. Adjust optional configuration entries. For more information about these and other configuration variables, see *Configuration Reference for Oracle WebCenter Content*:

   - `NotificationQuery`: Defines the criteria for the automatic query that searches for expired content.
   - `NotifyExtras`: Defines the users who receive a list of expired content.
   - `NotificationIntervalInDays`: Defines how often a notification query is run.
   - `NotifyTime`: Defines the time of day the query is run.
   - `NotificationMaximum`: Defines the maximum number of content items to be returned by the query.

   By default, an email message is sent to the administrator at midnight, seven days before a piece of content is set to expire. Additionally, an *Expired Content* link is added for the author and system administrator on their respective Content Management menus.

3. Restart Content Server.

4.4 Managing Revisions Using Repository Manager

A revision is a new or revised version of a content item. By default, revisions are numbered sequentially starting with Revision 1, and every time the content item is checked out and checked in again, the revision number is incremented by one and Content Server creates a new revision of that file. The new revision has the same content ID as the previous revision, but the native file and the metadata can be the same or different. The system stores the previous versions of a file, which can be reviewed as necessary.

This section discusses the following topics:

4.4.1 Check In and Check Out a Revision

To check in a new revision or check out a revision using the Repository Manager:

> **Note:**
>
> These tasks must be performed using the standalone application. For details on running standalone applications, see *Administering Oracle WebCenter Content*.

1. Start the Repository Manager in standalone mode.
2. Click the **Content** tab.
3. Select the item to be revised.

4. Click **Functions** then **Add Revision** or **Check Out**. You can also right-click and choose the appropriate option.
5. On the Add New Revision page or Check Out Item page, enter the information for the revision to be checked in.
6. Click **OK**.

4.4.2 Undoing a Check-Out or Resubmitting a Revision

To undo a check-out or resubmit a revision using the Repository Manager:

1. From the main menu, choose **Administration** then **Admin Applets**.
2. Choose **Repository Manager** then the **Content** tab.
3. Select one or more revisions to use.
4. Choose **Functions** then **Undo Check Out** or **Resubmit**. You can also right-click and select the appropriate option.
5. To exclude a revision from the list, clear the check box next to the revision.
6. Click **OK**.

4.4.3 Deleting Revisions

To delete a particular revision using the Repository Manager:

1. From the main menu, choose **Administration** then **Admin Applets**.
2. Choose **Repository Manager** then the **Content** tab.
3. Select one or more revisions to delete.
4. Click **Delete Revision**. You can also choose **Functions** then **Delete Revision**, or right-click and select **Delete Revision**.
5. To exclude a revision from the list, on the Delete Revision page, clear the check box next to the revision.
6. Click **OK**.

To delete **all revisions** of a content item follow the same steps, choosing **Delete All Revisions** from the appropriate menus.

4.4.4 Managing Workflow Revisions

A workflow specifies how content is routed for review and approval before it is released to the system. Users are notified by email when they have a file to review.

From a workflow participant's point of view, there are two types of workflows:

- A **basic** workflow defines the review process for specific content items, and must be initiated manually.
- In a **criteria** workflow, a file enters the workflow automatically upon check in when its metadata matches predefined criteria.

When a workflow revision is approved using the Repository Manager, any approval steps in the workflow are bypassed. The workflow may complete normally, but bypassing approval steps can have unanticipated consequences. For example, if a workflow step requires an electronic signature and the associated revision is approved

through the Repository Manager, there will be no record of an electronic signature, even though the workflow completes and the revision is approved.

> **Note:**
>
> Be sure you understand the consequences of approving a workflow revision using the Repository Manager before doing so.

To approve or reject a revision in a workflow using the Repository Manager:

1. From the main menu, choose **Administration** then **Admin Applets**.
2. Choose **Repository Manager** then the **Content** tab.
3. Select one or more revisions to approve.
4. Choose **Functions** then **Approve** or **Reject**. You can also right-click and choose **Approve** or **Reject**.
5. To exclude a revision from the list, clear the check box next to the revision.
6. Click **OK**.

4.5 Subscribing to Content

A subscription is a function that notifies users by email when a particular content item has been revised.

An email message buffer is 20000 bytes. If a large number of subscription email notices are sent at one time (for example, 40 content items with 40 subscribers each), the buffer can be overloaded and the email messages are not sent. The limit to the total size of a subscription notification email sent is 1 GB. The total number of subscription notification emails that can be included in one email sent to *n* users is 1 GB divided by the size of the subscription notification email.

> **Tip:**
>
> To change the subscription notification message, use Component Architecture to customize the following:
>
> - subscription_mail_subject include (in `std_page.htm` file)
> - wwSubscriptionMailSubject string (in `ww_strings.htm` file)
> - `subscription_mail.htm` template

Create subscriptions in two ways:

- **Basic subscription:** Users manually subscribe to individual content items. This type of subscription is predefined.
- **Criteria subscription:** Users can subscribe to a group of content items based on metadata criteria. Administrators can set up a Criteria subscription in two ways: with users or with aliases. If a subscription is set up with users, users can unsubscribe if they want. If aliases are used, users cannot unsubscribe.

Subscribe to content items in two ways:

- **Open subscription:** Users voluntarily subscribe to a content item through a Basic or Criteria subscription.
- **Managed subscription:** An administrator assigns users and aliases to a particular subscription. If individual users are assigned, each user can unsubscribe if they want. If an alias is assigned, the users in that alias cannot unsubscribe.

These are common tasks in managing subscriptions, as discussed in the following sections:

- Adding or Editing a Criteria Subscription
- Adding or Unsubscribing Users
- Viewing Subscription Information
- Deleting a Criteria Subscription

4.5.1 Adding or Editing a Criteria Subscription

To specify subscription criteria:

1. From the main menu, choose **Administration** then **Admin Applets**.
2. Select **Repository Manager** then the **Subscription** tab.
3. Click **Add**.
4. On the Add/Edit Subscription Type page, enter the subscription information:

> **Important:**
>
> If criteria fields are changed, all current subscriptions are deleted. Use care when working with this feature.

   - Name: Name for the subscription.
   - Description: A brief description.
   - Notifications: If selected, enables email notifications to users.

     The `PrimaryWorkQueueTimeout` configuration variable sets the number of seconds until workflow and subscription notification emails are sent. For more information about configuration variables, see *Configuration Reference for Oracle WebCenter Content*.
   - Criteria fields: To add fields, click **Fields**. On the Fields page, select the boxes of fields to be used as criteria for triggering the subscription. The values for these fields are set later when users are added.
5. Click **OK**. Confirm enabling the subscription.

4.5.2 Adding or Unsubscribing Users

This section describes how to add or unsubscribe users.

> **Tip:**
>
> If any of the users added to subscription do not have a correct email address, notification fails. The system quits after it encounters five errors in the work queue log and does not notify the rest of the subscribers.

4.5.2.1 Adding users to a Criteria subscription

To add users to a Criteria subscription:

1. From the main menu, choose **Administration** then **Admin Applets**.
2. Select **Repository Manager** then the **Subscription** tab. Select the subscription to use.
3. Click **Subscribers**.
4. On the Users Subscribed page, click **Add**.
5. On the Add Subscription page, select **User** or **Alias** then click **Select**.
6. On the Select User page or Select Alias page, choose the users or aliases to be subscribed.
7. Click **OK**.
8. Set the values for the criteria fields specified earlier.
9. Click **OK**.

4.5.2.2 Unsubscribing users

To unsubscribe a user:

1. From the main menu, choose **Administration** then **Admin Applets**.
2. Select **Repository Manager** then the **Subscription** tab.
3. Select the subscription to use.
4. Select the revision to unsubscribe.
5. Click **Function** then **Subscribers**, or right-click and select **Subscribers**.
6. On the Subscribers page, select the user alias to unsubscribe.
7. Click **Unsubscribe**.
8. On the confirmation page, click **OK**.

4.5.3 Viewing Subscription Information

To view subscription information for a revision using the Repository Manager:

1. From the main menu, choose **Administration** then **Admin Applets**.
2. Select **Repository Manager** then the **Subscription** tab.
3. Select the subscription to use.
4. Select the revision to view the subscription information for.
5. Select **Functions**, **Subscribers**, or right-click and select **Subscribers**.

6. To narrow the Subscriptions list, on the Subscribers page:
   a. Select the **Use Filter** check box.
   b. Click **Define Filter**.
   c. On the Subscription Detail page, enter the filter criteria.
   d. Click **OK**.
7. To view all subscription details for a particular user or alias, select the user or alias and click **View Details**.

   The Subscription Detail page opens.

4.5.4 Deleting a Criteria Subscription

To delete a Criteria subscription:

1. From the main menu, choose **Administration** then **Admin Applets**.
2. Select **Repository Manager** then the **Subscription** tab.
3. Select the subscription to use.
4. Select a subscription.
5. Click **Delete**.
6. On the confirmation page, click **Yes**.

4.6 Signing Content Electronically

Electronic signatures are used and managed in several different contexts:

- **Workflow**: Used to specify that a particular step requires an electronic signature for approval.

  Because electronic signatures are stored separately from both the content item and from its metadata, multiple users can sign a particular content item revision. For more information about using electronic signatures in workflows, see Managing Workflows.
- **Content Item:** Used to sign a content item electronically and compare a local file against a signed content item (or against all repository content) to see if the local file matches. For more information, see *Using Oracle WebCenter Content*.
- **PDF Watermark:** Used to apply a watermark that uses electronic signature metadata.

This section discusses the following topics:

- About Electronic Signatures
- Custom Electronic Signature Metadata
- Adding or Editing a Custom Electronic Signature Field
- Configuring Electronic Signatures

4.6.1 About Electronic Signatures

An electronic signature is a unique identifier computed from the binary content of a content item and associated with other metadata such as the name of the user who signs the content item. Unlike a digital signature, which uniquely identifies both the document and the signer and encrypts the information with the document, an electronic signature is not stored with the document.

When a content item is checked in, Content Server generates the identifier and stores it with the revision metadata for the content item. When a content item is signed, a copy of the identifier is stored with the electronic signature metadata. When a modified revision of the content item is checked in, a new identifier is calculated.

Content Server can compare the identifier stored with the content item to the identifier stored with the electronic signature to help determine if a signed content item has changed and if existing signatures for a content item are valid.

> **Note:**
>
> The identifier is computed from the content only, not the associated metadata. A change in the metadata for a content item does not invalidate the electronic signature for the content item.

Because electronic signatures are stored separately from both the content item and from its metadata, multiple users can sign a particular content item revision. For example, in a workflow approval process, multiple reviewers may sign a revision of a content item. For more information, see Managing Workflows.

Any user with access to the Document Information page for a content item can sign the content item. For more information about signing a content item, see *Using Oracle WebCenter Content*.

When using the Archiver with the Electronic Signatures component, use the table archive feature to move the ElectronicSignatures table. If archived content is restored without the associated signature metadata, errors can occur. For more information about archiving content, see *Administering Oracle WebCenter Content*.

When Electronic Signature is enabled along with PDF Watermark, the PDF Watermark capabilities are enhanced to provide the ability to apply a watermark of selected electronic signature data on a PDF rendition of a document. For more information, see Add or Edit an Electronic Signature Watermark.

4.6.2 Custom Electronic Signature Metadata

When a content item is signed electronically, the signature includes standard metadata about the user, such as the user name and password, and metadata about the content item itself, such as the name (dDocName) and revision (dRevisionID). The Electronic Signature component also provides the xESigHasElectronicSignatures field which is automatically set to 1 (true) when a content item is signed.

Metadata fields that are stored as part of the metadata for the electronic signature can also be defined. Electronic signature information is stored and managed in a separate ElectronicSignatures table in the database.

When creating a custom metadata field, select a basic data type, and optionally specify a choice-list of comma-delimited values, and designate one or more fields as required fields. The defined fields are displayed when the user signs a content item and when the user displays detailed signature information about a content item. For more information about these pages, see *Using Oracle WebCenter Content*.

4.6.3 Adding or Editing a Custom Electronic Signature Field

Consider metadata requirements carefully before creating custom metadata fields. After creating a field (click **Save Changes**), the field name, the data type, or the required status cannot be changed. The field must be deleted and a new field created in order to delete it. When a custom field is deleted, any stored data associated with that field is also deleted.

To create or edit a custom Electronic Signature field:

1. From the main menu, choose **Administration** then **Electronic Signatures**.
2. To add a new field, on the Electronic Signatures Configuration page, click the **Add New Field** icon (the green plus sign).
3. Specify an internal field **Name**. This is the field name in the data table.

   Duplicate names are not allowed. Maximum field length is 29 characters. Use only letters, numbers, and underscores (_). The name must start with a letter. Do not use special characters.
4. Specify a **Display Label**. This is the label displayed for the field on pages and dialogs.
5. Specify a data type. The default data type is **Text**.
6. To specify a choice list for a field, select the check box in the associated **Choice List** column and specify the choices as a comma-delimited list of values.
   - The values must match the data type selected for the field.
   - Values are displayed in the specified order on pages. The first value in the list is the default value.
   - To provide no default value, enter a space followed by a comma as the first value in the choice list.
7. To specify that the custom field is itself a check box, select **Checkbox**. A check box field is automatically designated a required field. The user must select the check box to complete the electronic signature.The Display Label field contains acknowledgement text to display next to the check box.
8. To specify that the user must supply a value in the associated field to complete the electronic signature, select **Required**.
9. Repeat steps 2 through 8 for each field to add.
10. Fields are displayed on pages in the order listed in this table. To change the order of one or more fields, select the check box next to the field or fields and use the Move Up and Move Down icons at the top of the table to move the fields up or down in the order.

11. To delete one or more field from the table, select the check box next to the field or fields and use the Delete Fields icon to remove the field or fields and all associated field data. Fields are not permanently deleted until **Save Changes** is selected.
12. To commit the changes, click **Save Changes** then click **OK** on the confirmation page.

4.6.4 Configuring Electronic Signatures

By default, the Electronic Signatures component requires that Secure Socket Layer (SSL) security be enabled when applying electronic signatures to prevent the possible interception of password information in otherwise unsecured network transmissions.

For some applications, such as workflow sign-off on a secure company intranet, the requirement adds additional overhead that may not be necessary.

To disable the SSL requirement for Electronic Signatures, set the DisableESigSSLCheck configuration variable in the config.cfg file to True:

```
DisableESigSSLCheck=true
```

For information about setting configuration variables, see *Configuration Reference for Oracle WebCenter Content*.

The electronic signature authentication process redirects users to the Oracle WebLogic Server login page before they can sign content items.

The Sign Content Item page has a time-limit cookie, default is 2 minutes, for reauthenticating users before signing content items. You can specify the timeout by setting the ESigCookieTimeOut property (with the value in seconds) in the electronicsignatures_environment.cfg file.

For example, to set the cookie timeout value to 30 seconds, specify the following:

```
ESigCookieTimeOut=30
```

4.7 Managing Native Content Conversion

> **Note:**
>
> Unless Content Server is configured to work with an Inbound Refinery instance, files are all passed through to the website in their native format.

When Content Server is configured as a provider for an Inbound Refinery instance, you must specify what file formats to pass to the refinery for conversion, based on the file extension. You can do this in the following ways:

- You can use the File Format Wizard, accessed from the Refinery Administration folder in the Administration tray
- You can use the File Formats option of the Configuration Manager applet to map file extensions (`.doc`, `.txt`, and so on) to file formats and then map the file formats to the conversion option on the refinery. This option provides more flexibility in mapping different file extensions to different conversion options

- You can create a custom component to base the conversion on the value of specified metadata fields for the content item, including the file format or custom fields.

After the job passes from Content Server to Inbound Refinery, the refinery configuration determines how to convert and return the native file.

File formats are automatically configured during installation or can be added and changed as needed.

For more information about conversions, see Managing Content Conversion.

- Identifying MIME Types
- Native Applications Requirements for Content Conversions
- Associating File Types with Conversion Programs
- About Thumbnails

4.7.1 Identifying MIME Types

When you define new file formats, specify the MIME (Multipurpose Internet Mail Extensions) type corresponding to the file extension (for example, the format mapped to the `doc` file extension is application/msword).

When a content item is checked in to the repository, the content item's format is assigned according to the format mapped to the file extension of the native file. If the native file is not converted, Content Server includes this format when delivering the content item to clients. Using the MIME type for the format assists the client in determining what type of data the file is, the associated helper applications, and so on.

Check MIME types and the list of registered MIME types at `http://www.iana.org/assignments/media-types/index.html`.

4.7.2 Native Applications Requirements for Content Conversions

Oracle WebCenter Content Inbound Refinery supports using Microsoft Office Suite 32-bit installations for the greatest compatibility. Using 64-bit installations of Microsoft Office Suite is not supported. Microsoft Office Suite 32-bit is the default installation and is recommended by Microsoft for compatibility with third-party extensions. For more information, visit `http://office.microsoft.com` and search for articles HA010369476, HA102840825, and ee681792.

The native applications used to convert content must meet the following requirements.

Native Application	Requirements
MS Word MS Project MS Excel MS PowerPoint MS Visio	Verify that the native application is installed if needed by Inbound Refinery for the conversion. Associate the file type to a conversion process on the **File Formats** tab. For Word and PowerPoint applications, use the **Native Options** tab on the Local Inbound Refinery Configuration page to specify whether to process links.

Native Application	Requirements
MS Publisher FrameMaker PhotoShop PageMaker InDesign	Verify that the native application is installed. Associate the file type to a conversion process on the **File Formats** tab.
Other	Verify that the native application is installed (if required). Install the custom conversion program in Inbound Refinery. Associate the file type to a conversion process on the **File Formats** tab.

4.7.3 Associating File Types with Conversion Programs

Associating file types with conversions is a two-stage process.

4.7.3.1 Adding file format and associating file extension

To add the file format and associate the file extension with the format:

1. From the main menu, choose **Administration** then **Admin Applets**.
2. Click **Configuration Manager.**
3. On the Configuration Manager page, choose **Options** then **File Formats** from the Page menu.
4. On the File Formats page, click **Add** in the File Formats pane to add a file format.
5. On the Add/Edit File Format page, enter the necessary information:
   - Format: Usually the MIME type.
   - Conversion type: Associates the format name with a conversion.
   - Description: A brief description of the file format.
6. Click **OK**.

4.7.3.2 Adding a file extension

To enter the file extension to associate with the format:

1. Click **Add** in the File Extensions pane.
2. On the Add/Edit File Extension page, enter the necessary information:
   - Extension: The designation for the file format. A file with this format is converted using the conversion specified by the Map to Format field.
   - Map To Format: A list of the available formats with specified conversions (defined in the File Formats pane). Select a format to directly relate all files with that extension to a specific conversion program.
3. Click **OK**.

4.7.4 About Thumbnails

Thumbnails are small preview images of content. They are used on search results pages and typically link to the web-viewable file they represent. This means that users do not need to rely solely on text information such as the title to tell if a file is the one for which they are looking. A thumbnail provides consumers with a visual sample of a file without actually opening the file itself. This enables them to check a file before committing to downloading the larger, original file.

You can automatically generate thumbnails for supported file types with options provided by Content Server.

Content Server provides a basic set of thumbnail creation options. Oracle WebCenter Content: Inbound Refinery provides a more extensive set of options for file conversion and thumbnail generation.

4.8 Defining Content Types

Files are grouped in directories designated by *content types*.

- Content types become the names of the subdirectories in which documents are stored in the `weblayout` and `vault` directories.
- Content types can correspond to departments (such as ENG, MKTG, and HR), document types (such as MEMO, FORM, and SPREADSHEET), or any other model needed.
- Several content types are defined by default (Document, Binary, Digital Media, and so on), but you can modify or delete these.
- Each content type is assigned an image, which helps users identify the content type on search result pages. Several images are provided or you can create and assign your own images.
- Create a manageable number of content types, typically no more than 50. Too many content types increases the amount of effort required to maintain the system, and makes it difficult for contributors to assign the correct content types to their files.
- When configuring content types, consider using the same prefix in a content type when grouping similar information. For example, the prefix MEMO is used in the following content types: MEMO_INT, MEMO_EXT, MEMO_EXEC.

4.8.1 Creating, Editing, or Deleting a Content Type

Use this procedure to:

- Create a new content type
- Edit an existing type
- Delete a content type

1. From the main menu, choose **Administration** then **Admin Applets**.
2. Click **Configuration Manager.**
3. On the Configuration Manager page, choose **Options** then **Content Types** from the Page menu.

4. To add a new type, on the Content Types page click **Add**.

   To edit a type, highlight the type name and click **Edit**.

   To delete a type, highlight the type name and click **Delete**.

   > **Note:**
   >
   > You cannot delete a content type if content still exists with that type. Make sure no content is using the type before attempting to delete it.

5. On the confirmation page, click **OK**.
6. On the Add/Edit Content Type page, enter or edit the name and description of the type.
7. Select an image from **GIF** list to associate with the content type.
8. Click **OK**.

5
Organizing Content

Oracle WebCenter Content provides several ways to organize content. The Folders feature provides a hierarchical folder interface, similar to a conventional file system, for organizing and locating some or all of the content in the repository. The Contribution Folders feature provides similar functionality, however, Folders is a scalable, enterprise solution and is meant to be a replacement for Contribution Folders. WebDAV (Web-Based Distributed Authoring and Versioning) provides a way to remotely author and manage Oracle content using clients that support the WebDAV protocol. Content Folios is an optional feature that provides a quick and effective way to assemble, track, and access logical groupings of multiple content items from within the secure environment of Content Server.
This chapter discusses the following methods of organizing content:

- Managing Folders
- Managing WebDAV
- Managing Content Folios

5.1 Managing Folders

The folder hierarchy provided by Folders is accessible through both the standard content management Web interface and through the WebDAV interface. With the standard interface, folders and content items (files) are accessed with a browser and specially designed Web pages. With the WebDAV interface, a network connection is made to Content Server and then folders and files are accessed through Windows Explorer, just as shared folders are accessed. Folders is supported by the FrameworkFolders component in Content Server.

This section discusses the following topics:

- Understanding Folders
- Configuring Folders
- Working with Retention Scheduling

5.1.1 Understanding Folders

The familiar folder and file model provides a framework for organizing and accessing content stored in the repository. Functionally, folders and files are very similar to those in a conventional file system. Folders and files can be copied, moved, renamed, and deleted. Shortcuts can be created in order to access a content item from multiple locations in the hierarchy.

Files in the Folders interface are similar to symbolic links or pointers to content items in the repository. The operations performed in the Folders interface, such as searching or propagating metadata, effectively operate on the associated content items.

Users can create and edit folders, shortcuts to folders, and links to documents as allowed by Content Server's standard security model. Folders are assigned security attributes in the same way they are assigned to content items, including security group, account, and Access Control List attributes, if enabled.

By default, folders inherit the security settings and other default metadata defined for the parent folder. Security and metadata values can be set for a given folder and those values propagated to folders and content items within the folder.

This section discusses the following topics:

- Folders and Files
- Shortcuts and Links
- Query Folders and Searches
- Folders Retention
- Personal Folders
- Folders Metadata
- Versioning

5.1.1.1 Folders and Files

Users can easily view the relationship between folders and subfolders and can browse to a group of content items. Using Folders, users can perform the following actions with the privileges defined by Content Server's standard security model:

- Browse to locate content items for check-in, check-out, and to view and change folder and item information.
- Create new folders and subfolders.
- Create new content items in a folder or add existing repository content to a folder.
- Add shortcuts to folders or content items in one or more locations. Shortcuts act as placeholders for the referenced content item.
- Move or copy folders or files to other locations.
- Rename a folder or file.
- Remove a file from the folders hierarchy. This does not affect the associated content item.
- Delete a folder or file. When deleted, the folder or file and any shortcuts to it are removed from the folders hierarchy. Any content items associated with the files are set to *expired* in the repository.
- Make a folder ReadOnly. Making a folder read only prevents renaming, moving, or deleting the folder; however, content can still be checked into the folder.
- Create a query folder that contains content items returned by the query associated with the folder. For more information about query folders, see Query Folders and Searches.
- Create a retention query folder and assign retention rules for the content items returned by the query. For more information about query folders and retention scheduling, see Folders Retention.
- Assign folder security and values for content items created in the folder. Specified metadata values can be propagated to the contents of a folder or propagation can be blocked for a given folder. For more information, see Versioning.

The Folders interface follows several conventions familiar to users of file systems:

- Use standard Windows naming conventions when creating folders. Do not use the following characters:

  ? #& /*" |< > :^

- Content Server can store multiple files of the same name as separate content items. However, in the Folders interface, file names in a given folder must be unique (in the same way that a folder in Windows cannot contain two files with the same name).

5.1.1.2 Shortcuts and Links

With Folders, the same folder or content item can be referenced in multiple locations using shortcuts that act as placeholders for the referenced folder or file. Shortcuts to folders or files can help locate and manage the target content items within the folder hierarchy.

Folders and folder shortcuts are identified with different icons.

Icon	Description
	Folder: Folders can contain other folders, content items, and shortcuts to other folders and content items. Folders are identified by a standard folder icon.
	Folder Shortcut: A folder shortcut includes the contents of the associated folder in the hierarchy at the point where the shortcut is stored. Folder shortcuts are identified by a folder icon with an arrow and can reference either a folder or a query folder. Folder shortcuts are excluded from metadata propagation actions.
	Query Folder: The contents of a query folder are the repository content items returned by the query associated with the folder. Query folders are identified by a folder icon with a magnifying glass.
	Retention Query Folder: Similar to a query folder, the contents of a retention query folder are the repository content items returned by the query associated with the folder. Retention rules can also be set for the content items returned by the query. Retention query folders are identified by a folder icon with a magnifying glass and a clock.

Content items in the Folders interface are similar to links to items in the repository. There are two types of links for content items.

Icon	Description
	File (primary link): There can be only one primary link to a content item in the Folders interface. The primary link represents the content item in the repository and is identified by a standard document icon. In most respects, working with a file (or primary link) is the same as working directly with the content item in the repository. For example, the status of the associated content item for a deleted file is set to "expired."

Icon	Description
	Shortcut (secondary link): There can be any number of file shortcuts in the Folders interface to an associated content item. A file shortcut is identified by a document icon with an arrow indicating that it is a reference to the actual content item. Shortcuts are excluded from metadata propagation actions. Changes made by means of the shortcut (such as metadata changes) are made to the underlying content item. Changes made to the shortcut itself (such as deleting the shortcut) do not affect the underlying content item.
	Query result: The contents of a query folder are the repository content items returned by the query associated with the folder. Query content items are identified by a document icon with a magnifying glass.

5.1.1.3 Query Folders and Searches

A query folder functions much like a saved search. Each time is it accessed, the query associated with the folder is initiated. The contents of a query folder are the content items returned by the query. The contents of query folders can change dynamically as the contents of the repository change.

Query folders contain the actual repository content items returned by the query, not the folders and shortcuts. Query folder contents can be copied, viewed, and updated for individual items, or metadata changes can be propagated through all items in the query folder.

Folders also expands the standard search results options to include the **Create Query Folder** option to save a search query as a query folder. To search for folders or files from within a folder, use the options in the **Search** menu in a given folder. You can search any or all folder metadata fields.

5.1.1.4 Folders Retention

Basic content retention scheduling can be done by creating a retention query folder, assigning retention attributes to the folder, and then configuring the retention schedule. Retention rules can be assigned based on the age of the content item or on the number of revisions. If you have Records installed and the full functionality enabled, retention rules based on categories defined in Records can be established.

Administrative privileges are needed to specify retention rules or schedules. For information about specifying retention scheduling, see Specifying Retention Rules. For information about specifying retention scheduling, see Configuring a Query Retention Schedule.

Considerations

The following considerations apply to retention query folders:

- Retention rules are associated with the retention query folder but are stored separately from the standard folder metadata. For this reason, you cannot search for a query folder based on the folder's retention attributes.
- Unlike standard query folders, retention query folders search only database values and cannot perform full-text searches even if full-text search is supported.

- If multiple retention rules are specified for a particular retention query folder, all the rules must be satisfied for the disposition to occur. For example, if you specify the age as 1 calendar year and the number of revisions to keep as 3, only those items that are more than 1 year old and that are older than the last three revisions are deleted.
- Different queries can include the same content item in their results. In this case, the retention rules for each retention query folder are applied independently from one another. For example, if one query folder specifies the number of revisions to keep as 2 and another specifies the revisions to keep as 3, only two revisions of the item are retained.
- Folders retention is treated differently than that in Records. When using Records, if multiple delete actions are called, the retention with the longest interval is used. In Folders, the shortest interval always runs first.
- Folders retention processes items based on the values in the dCreateDate row in the Revisions table in the database.

Considerations with Records Usage

If both Folders and Records are used on the same system, the following additional considerations apply:

- If Records is installed, it is possible to have two retention schedules (as well as multiple rules) for the same item. If a content item has retention rules defined in both Content Server and in Records, only the retention and schedule defined by the Records system are used.
- If Records is installed with a level of DoD Baseline or higher, retention query folder options are not available in the Content Server interface. Any existing retention query folders retain their icon and (inactive) retention attributes, but function as a standard query folder.

  If the level is then set to Standard or lower, then retention query folder options are enabled in Content Server and the rules for any existing retention query folders become active.

5.1.1.5 Personal Folders

In the root folder of the Folders hierarchy is a Users folder that contains a folder defined for you as an authenticated user. You can create subfolders and content items in the same way you do with other folders in the hierarchy. Every authenticated user can have a personal folder.

Folders provides menu options to quickly add folders, files, and shortcuts to your personal folder, referred to as **Add to My Folder** in menus. Although your personal folder is visible only to you, the items in the folder are governed by the security settings for the item itself and not necessarily those of the enclosing folder. Some items may be accessible to other users, for example, in search results.

To access your personal folder, use the main menu to choose **My Content Server** then **My Folders**.

5.1.1.6 Folders Metadata

Every folder has a set of metadata values that can be applied to content items added to the folder. Folders can be configured to enforce metadata rules on their content items or to allow any or all values to be modified. For example, a folder could be configured to enforce 'Secure'

as the value for the Security Group metadata field. Then, when a content item is added to that folder, the Security Group value automatically updates to Secure.

Folders inherit the default metadata assigned to their parent folders unless the folder is explicitly configured otherwise. Subsequent changes to a parent folder's metadata do not affect the metadata for existing subfolders unless explicitly propagated down through the hierarchy.

Folder metadata inheritance and propagation make it easy to apply metadata to content items. Whether you are an administrator managing all folders and files or a user managing your own folders and files, it is a good idea to plan a metadata strategy before creating folders and adding content items. The strategy should include the following basic steps:

1. Determine whether specific folders or branches in the hierarchy have unique metadata requirements and how best to identify and manage those requirements.
2. Determine which metadata fields (if any) a user should specify when adding or checking in a content item through a particular folder.
3. Determine which metadata fields (if any) should have a default value or an enforced value for a particular folder.
4. Determine which subfolders (if any) are eligible to be changed when propagating metadata through a folder.
5. Determine whether to use profiles to manage metadata requirements. An administrator can create one or more profiles to organize, selectively display, and control access to metadata fields based on rules associated with the profile.

Default metadata values are automatically applied to new content items created in or checked in to a folder. To modify the default metadata values for a folder, Delete permission to the folder is required or you must be the author and have Write permission.

> **Note:**
>
> Specifying a default value for the Author field will limit the users who can check documents into the folder. Only users with Admin permission to at least one group will be able to check documents into a folder for which a default author is specified.

Default metadata values are also used as the default values when propagating metadata.

If Oracle WebCenter Content: Desktop is used and the folder has the **Prompt for Metadata** option selected, you are prompted to provide metadata values for the item rather than relying on the folder's default metadata settings.

Content items in a folder do not necessarily have the same security settings. To propagate metadata to content items, you must also have Write permission for the content item. To restrict changes to folders only, select the **Propagate To Folders Only** option.

When propagating metadata, select the metadata fields and specify the values to propagate from the metadata available for the current folder. Any metadata value that can be changed can be propagated. For example, you can propagate the Security

Group or Owner values, but you cannot propagate the Content ID. Blank field, such as the Comment or Expiration Date fields, can be propagated to clear the associated values from content items.

To prevent propagation, select **Inhibit Propagation** in the folder information for a folder or override a folder's inhibit setting using the **Force Propagation** setting on the Propagate page.

An administrator can create sets of metadata as one or more profiles that the administrator or other users can easily apply to folders when specifying folder defaults or when propagating metadata.

5.1.1.7 Versioning

Content items can be checked in and out through the Folders interface in much the same way as through the standard content management pages. When a particular content item is viewed or edited, options are available to check out the item and then check in a new version of that item.

Folders provides two modes for viewing content item versions:

- Published Items (consumption mode): The latest released revisions of documents are displayed. These are the same revisions that are returned in search result listings.
- All Items (contribution mode): The latest revision of each document is displayed. These can include the revisions of documents that are still in workflow or have otherwise not finished with the search indexing process.

Users can switch between the two modes to see released content items only or to see content items that require work before being released. The selection remains in effect until changed.

5.1.2 Configuring Folders

Different types of configuration variables can be set to configure the FrameworkFolders component:

- Folder Variables
- Folders Migration Variables
- Folders WebDAV Variables

5.1.2.1 Folder Variables

These variables can be used to configure optional settings in the Folders interface.

Variable	Description
`AuthorDelete`	If set to true, the owner/author of an item can delete the item as long as they have Read privilege, otherwise, they require Delete privilege. The default value is true.

Variable	Description
DisableFolderRestrictions	If set to true, allows browsing of the Users folder (FLD_USERS), otherwise when a user tries to access the Users folder, they are redirected to their personal folder (FLD_USER:<username>). The default value is false. If explicitly set to true in the config.cfg file, all users can see the contents of the Users folder. An administrator can temporarily set the value as a binder variable in the URL when browsing the Users folder.
DisablePersonalFolderFormat	Set to true to disable personal folder naming specified by FldPersonalFolderFormat. The default is false. If the name format for personal folders is changed or disabled after personal folders are created, the existing folders must be manually renamed, or recreated. For example, if the personal folder for user abc.def@example.com is formatted with the name abc.def and then DisablePersonalFolderFormat is set, the database retains the existing folder name, but the user interface expects it to be named abc.def@example.com. You must rename the folder to match the disabled formatting or delete the row from the database and recreate the folder when the user logs in.
FldDefaultFilesLoadCount	Number of files to display in the folder explorer. The default is 50.
FldDefaultFoldersLoadCount	Number of folders to display in the folder explorer. The default is 50.
FldEnableInProcessIndicator	If set to true, enables the Process Indicator shown during copy, move, delete, and propagate operations. The default value is false.
FldPersonalFolderFormat	Specify the regular expression used to construct the name of the personal folder from the user's name. By default, the regular expression is (.+)@(.+):$1 (two groups of one or more characters separated by "@" and using the first group as the folder name. For example, the user name abc.def@example.com results in a personal folder is named abc.def. For information about regular expressions, see http://download.oracle.com/javase/6/docs/api/java/util/regex/Pattern.html.
FldShowAutoPropagateOption	By default, moved items retain the metadata defined for the item and do not inherit metadata values in the new location. If set to true, the **Auto propagate destination's metadata to folder** option is added to the Choose a Destination window for mover operations. If the user selects this option, moved items inherit the metadata defined by the enclosing folder in the same way that copied items do. The default value is false.
FoldersDefaultDocType	Specify a document type to use if the document type cannot be determined when creating a content item. The default document type is Document.
FoldersIndexParentFolderValues	Enables subfolder searching if Oracle Text Search is in use. The default is true. When enabled, the system adds all paths to all documents to the search index. Documents are re-indexed whenever they are added to or removed from a folder. In addition, the document is re-indexed if its full path changes in any way (for example, when the parent folder is moved).

5.1.2.2 Folders Migration Variables

These variables can be used to configure optional settings in the Folders Migration utility. The Folders Migration utility migrates folder content and structure from Contribution Folders (supported by the Folders_g component) to Folders (supported by the FrameworkFolders component). The utility is available when the tables associated with Contribution Folders are present in the database schema.

Variable	Description
`FldMigrateDefaultSecurityGroup`	Specify the default Security Group to assign to migrated folders if one is not already associated with the folder. If not set explicitly, the default value is Public. Contribution Folders do not need and may not have a Security Group setting. Migrated folders require a security setting.
`FldMigrateRootBaseName`	Specify the base name for the root folder created during migration. The folder name has the form: <$FldMigrateRootBaseName$>_<$date$>_#<run_index> If not set, the base value defaults to "Migrate".
`FolderMigrateExcludeList`	Specify the list of folders to exclude from the migration. The list may include folder IDs and folder marks. If not set explicitly, only the TRASH folder is excluded.
`ShowFolderMigrationMenu`.	Set to 0 (zero) to prevent the **Folder Migration** option from showing in the Administration menu. If set to 1 or if not set explicitly, and migration is possible, the option is displayed.

5.1.2.3 Folders WebDAV Variables

These variables can be used to configure optional settings in the Folders WebDAV interface.

Variable	Description
`OVERWRITE`	Set to false to prevent a WebDAV copy from writing over items with the same name. The default value is true

5.1.3 Working with Retention Scheduling

Content revisions can be disposed of based on the age of the content item or on the number of revisions. If Records is installed and full functionality enabled, retention rules based on Records categories can also be defined. For additional retention query folder considerations, see Folders Retention.

To define retention scheduling for the contents of a retention query folder, first specify the retention rules associated with the folder, then specify the retention schedule for each of the rules used with one or more retention query folder. This section discusses those tasks:

- Specifying Retention Rules
- Configuring a Query Retention Schedule

5.1.3.1 Specifying Retention Rules

Retention rules are specified when you create a retention query folder and can be modified at a later time. Retention rules can be specified for retention query folders only if you are an administrator. Retention query folders that do not include retention rules act like standard query folders.

> **Note:**
>
> If Records is installed with a level of DoD Baseline or higher, retention query folder options are not available in the Content Server interface. Any existing retention query folders retain their icon and (inactive) retention attributes, but function as a standard query folder.

The following procedure shows how to specify retention rules. For more information about creating folders and specifying queries, see *Using Oracle WebCenter Content*.

Query folders with retention rules apply the rules on a specified schedule. For more information about how to create a retention schedule for query folders, see Configuring a Query Retention Schedule. For details about setting up a Record retention schedule, see Managing a Records Retention Schedule.

1. Navigate to the folder where the retention query folder is stored.
2. To change metadata values, including the retention rules, choose **Update Folder Information** from the Actions menu for the associated folder.

   To change metadata values for the folder when you are viewing the contents of the folder, choose **Folder Information** from the Edit menu on the page.
3. Click **show advanced retention options**.
4. Choose one or more retention options. For example, to keep only the most recent 3 revisions of a content item, choose **Revisions** and specify **3**. Older revisions are deleted on the retention schedule specified for Revisions.
   a. **Revisions:** Specify how many revisions of the content items in the query folder to keep and click **Update**.
   b. **Age:** Specify how long to keep the content items in the query folder and click **Update**.

      If you have the full Records product, the units list includes fiscal units as well as calendar units.
   c. **Category:** Assign a category to the query folder and use the retention defined for the category to determine how to dispose of the content items.

      This option is available only with the full Records system.
5. Make any additional changes to the folder metadata or query and click **Save**.

5.1.3.2 Configuring a Query Retention Schedule

Query folders with assigned retention rules apply the rules on a specified schedule. A different schedule can be set for each type of retention rule. Content items that are

included in multiple query folders can have multiple retention rules, and therefore have multiple schedules applied to them.

Folders retention rules are treated differently than those in the Records system. When using Records, if multiple delete actions are called, the retention with the longest interval is used. In Folders, the shortest interval always runs first.

If a content item has retention rules defined in both Content Server and in Records, only the retention and schedule defined by the Records system is used.

To configure a query retention schedule:

1. From the Administration menu, choose **Folders Retention Administration** then **Configure Scheduled Jobs**.
2. On the Folder Retention Scheduled Jobs page, specify schedules for retention rules governed by age or revision.

   Age-based rules process items based on the values in the dCreateDate row in the Revisions table in the database.

   a. **Weeks/Days:** Select a Start Time and an End Time. This schedules the retention for query folders with Weekly retention rules. To run the scheduled disposition immediately, click **Run Now**.

   b. **Calendar Months:** Select a day of the month, a Start Time and an End Time. This schedules the retention for query folders with Monthly or Quarterly retention rules. To run the scheduled disposition immediately, click **Run Now**.

   c. **Calendar Years:** Select a month, a day of the month, a Start Time and an End Time. This schedules the retention for query folders with Yearly retention rules. To run the scheduled disposition immediately, click **Run Now**.

   d. **Fiscal Months/Fiscal Years:** If Records is installed, you can schedule the retention for query folders with Fiscal Month and Fiscal Year retention rules. To run the scheduled disposition immediately, click **Run Now**.

   e. **Retention Revisions:** Select a day of the month, a Start Time and an End Time. This schedules the retention for query folders with Revisions retention rules. To run the scheduled disposition immediately, click **Run Now**.

   > **Note:**
   >
   > If Records is installed and category retention rules are used, the categories are scheduled by their associated age or revision rules. For example, a category with a retention specified in months is governed by the value you specify here for **Calendar Months**. Likewise, to immediately apply the retention rules for all items with retention rules or categories specified in months, click the **Run Now** button associated with Calendar Months on this page.

3. Click **Update**.

5.2 Managing WebDAV

WebDAV is automatically installed and enabled with Content Server. It provides a way to remotely author and manage Oracle content using clients that support the WebDAV protocol.

For example, you can use Windows Explorer to manage folders and files or use Microsoft Office products to check in, check out, and modify content in the Oracle repository rather than using Oracle's Web browser interface. The WebDAV protocol is specified by RFC 2518.0. For more information, see the WebDAV Resources page at http://www.webdav.org.

> **Important:**
>
> WebDAV does not support the use of non-ASCII characters in user names.

For information about using the WebDAV interface, see *Using Oracle WebCenter Content*.

This section discusses the following topics:

- Understanding WebDav
- Configuring WebDAV

5.2.1 Understanding WebDav

WebDAV provides support for the following authoring and versioning functions:

- Version management
- Locking for overwrite protection
- Web page properties
- Collections of Web resources
- Name space management (copy/move pages on a Web server)
- Access control

When WebDAV is used with a content management system, the WebDAV client provides as an alternate user interface to the native files in the content repository. The same versioning and security controls apply, whether an author uses the Oracle Web browser interface or a WebDAV client.

In Content Server, the WebDAV interface is based on the folder interface provided by the Folders (FrameworkFolders) component. Except where noted, WebDAV functions similarly for both components.

This section discusses the following topics:

- WebDAV Clients
- WebDAV Architecture
- WebDAV Folders
- Multiple Concurrent Language Support

5.2.1.1 WebDAV Clients

A WebDAV client is any application that can send requests and receive responses using the WebDAV protocol. Typically, a WebDAV client requires no additional setup.

Although there are many applications that support the WebDAV protocol to some degree, Content Server is tested with, and supports the following:

- Microsoft Windows Explorer
- Microsoft Word 2002 (XP) through 2010
- Microsoft PowerPoint 2002 (XP) through 2010
- Microsoft Excel 2002 (XP) through 2010

Windows Explorer can be used to manage files created in a non-WebDAV client, but the native application cannot be used to check content in to and out of the repository.

> **Note:**
>
> Do not confuse the term WebDAV client with Oracle WebDAV Client, which is a separate Oracle product that enhances the WebDAV interface.

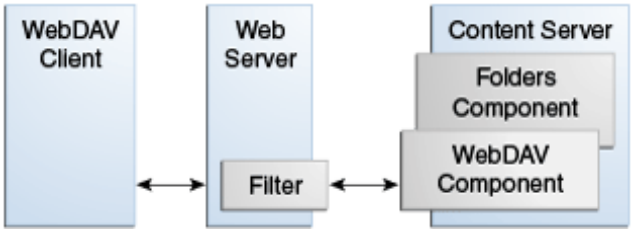
Oracle also offers Oracle WebCenter Content: Desktop, which can enhance the WebDAV client environment by more closely integrating with Windows Explorer, Microsoft Outlook, Lotus Notes, and other applications. For more information, see *Using Oracle WebCenter Content: Desktop*.

5.2.1.2 WebDAV Architecture

WebDAV support is implemented through a component which handles WebDAV requests directly. A WebDAV request follows this process (as illustrated in Figure 5-1):

1. The WebDAV client makes a request to Content Server.
2. The message is processed by the Web server through a custom filter.
3. On the Content Server, the WebDAV component performs the following functions:
   - It recognizes the client request as WebDAV.
   - It maps the client request to the appropriate WebDAV service call.
   - It converts the client request from a WebDAV request to the appropriate request.
   - It connects to the core Content Server and executes the request.
4. The WebDAV component converts the response into a WebDAV response and returns it to the WebDAV client.

Figure 5-1 WebDAV Process



> **Important:**
>
> WebDAV uses several nonstandard HTTP methods, including PROPFIND, PROPPATCH, MKCOL, DELETE, COPY, MOVE, LOCK, and UNLOCK. Many third-party applications-such as firewalls, proxy servers, load balancers, and single sign-on applications, do not allow these methods by default. If your network includes any of these applications, you may have to reconfigure them to allow the WebDAV methods.

5.2.1.3 WebDAV Folders

You connect to a WebDAV folder as you would a networked location. The credentials used are the same as those for the standard browser interface for Content Server. Folders and folder content can be used as defined by your user permissions. For example, if you have Read permission for a content item, you can view the file, but you cannot check in a revision to the file.

The WebDAV interface provides a subset of the options available through the browser interface. In general, users can create, delete, move, and copy content items and folders and modify and check in content items. To check out content items through the WebDAV interface, use a WebDAV client that can open the file. To perform other management tasks, such as specifying or propagating metadata values, use the standard browser interface.

For more information about creating a connection to a WebDAV folder and using WebDAV folders to manage content, see *Using Oracle WebCenter Content*.

5.2.1.4 Multiple Concurrent Language Support

To support multiple concurrent languages, certain WebDAV properties (metadata fields) should only contain characters that are viewable in all of the languages you intend to support. For example, in a multiple language environment that supports both English and Japanese, an English desktop would have trouble displaying Japanese (double-byte) characters.

In addition, different WebDAV clients provide different levels of support for characters within the ASCII character set. To ensure that WebDAV property fields can be displayed in your WebDAV client, the values in those fields must contain only characters that are supported by your client. For more information about character support for your WebDAV client, see the product documentation for your WebDAV client.

> **Note:**
>
> To ensure compatibility between languages and WebDAV clients in a multiple language environment, folder names and certain Content Server fields should only contain characters that can be displayed in all languages and in all WebDAV clients you intend to support. This is not a limitation of the Content Server fields themselves, but of the language mix and the WebDAV client environment.

Folder and File Names

It is recommended that you limit folder and file names to the printable ASCII character set (ASCII characters 32 to 128). In addition, folder and file names cannot contain the following characters:

? #& /*" |< > :

Microsoft Web Folders WebDAV Client

The following fields must conform to the compatibility standard you establish for your multiple language environment:

- the content name (dDocName)
- the original content name (dOriginalName)
- the content title (dDocTitle)
- the folder names

Oracle WebCenter Content Desktop WebDAV Client

The following fields must conform to the compatibility standard you establish for your multiple language environment:

- the content name (dDocName)
- the original content name (dOriginalName)
- the content title (dDocTitle)
- the content type (dDocType)
- the content item author (dDocAuthor)
- the security group (dSecurityGroup)
- the folder names

5.2.2 Configuring WebDAV

After installing WebDAV, most of the WebDAV system administration tasks can be done from folders Web pages.

This section discusses the following topics:

- WebDAV Connection Strings
- Default Content Item Naming
- Security and WebDAV

5.2.2.1 WebDAV Connection Strings

When creating a Content Server connection, the user must provide the WebDAV URL for that server. Each defined connection must have its own, unique WebDAV URL. Do not have two server connections on the computer that use the exact same WebDAV URL. The WebDAV URL typically has the following form:

```
http[s]://host-name:[port]/web-root/idcplg/webdav
```

For example:

```
http://server:7044/idc/idcplg/webdav
http://server.example.com:16200/cs/idcplg/webdav
https://server/cs/idcplg/webdav
```

With the use of a form-based login, WebDAV connection strings now require the `_dav` root before the web root. For example:

```
http://host_name:16200/_dav/cs/idcplg/webdav/
```

5.2.2.2 Default Content Item Naming

When users check new content in through a WebDAV folder, they cannot explicitly set metadata values such as the title for the content item. As a general rule, content items inherit any metadata defaults specified for the folder.

In the case of the content item title (dDocTitle), it is always set to the original file name (dDocOriginalName) except for Folders (FrameworkFolders component), if the folder specifies a title as part of its default metadata, the title specified by the folder is used as the document's title.

5.2.2.3 Security and WebDAV

The following security features are included in WebDAV:

- Access: The user logins and security controls in the folders component and Content Server also apply to content that is managed using WebDAV clients. For example, if you have Read permission for a content item, you can view the file, but you cannot check in a new revision to the file.
- Login Cookie: When a user logs in to Content Server through a WebDAV application, the WebDAV component sets a cookie in the client. The cookie remains set if a WebDAV request is made within the time specified by the `WebDAVMaxInactiveInterval` configuration parameter. The default is 3600 seconds, or one hour. The cookie remains set even if the WebDAV client application closes. If the cookie expires, the user must log in to Content Server again to perform WebDAV transactions through Microsoft Word, Excel, and PowerPoint.

  The cookie includes a cryptographic key that prevents unauthorized users from generating counterfeit cookies. The `WebDAVSecretKey` parameter is used to generate the key. To prevent WebDAV login cookies from being used on other Content Servers, change the `WebDAVSecretKey` setting to a new, unique value for each instance that is accessed through WebDAV.
- Windows Explorer: If a user logs in to Content Server through Windows Explorer, the client retains the user login authentication within the shell. Even if the login cookie expires, Windows Explorer sends the user name and password to Content Server automatically, so the user is not prompted to log in. The only way to clear this is for the user to log out of Windows.
- Personal Folders: Content Server creates a personal folder for each user (`/Users/username/`). The Web interface prevents users from creating folders in the `/Users` directory. To prevent users from having write access to the `/Users` directory through the WebDAV interface, however, you must explicitly set permissions for the `/Users` folder. For example, you can give most users Read access to the folder, and allow only administrators to write to the folder.

- Session timeout: If a WebDAV client does not specify a session timeout value, the default timeout specified by the `WebDAVDefaultTimeout` setting is used. If a file remains locked (checked out) for this amount of time with no activity in the session, an "undo check-out" is applied to any checked out content.

5.3 Managing Content Folios

Content Folios is an optional component that is automatically installed with Content Server. When enabled, it provides a quick and effective way to assemble, track, and access logical groupings of multiple content items from within the secure environment of Content Server. For example, you can assemble all items relevant to an upcoming brochure, such as images, logos, legal disclosures, and ad copy, and send them through a workflow process. After approval, you can download all associated content and send it for print.

This section discusses the following topics:

- Understanding Content Folios
- Creating and Using Content Folios

5.3.1 Understanding Content Folios

A content folio is an XML file checked in to the repository that uses elements to define a hierarchical structure of nodes, slots, and specified content items. In practice, a content folio is a logical grouping, or a framework in which to structure content. Simple folios are a flat container, while advanced folios can nest content in a hierarchy within folders. With an advanced folio, the hierarchy can be set before, during, or after content items are assembled.

Content can be added to existing folios or the folios can be locked so changes cannot be made. Items can be added by searching the repository. You can add content items to an advanced folio by checking new items into the repository or by searching for existing content. An advanced folio can also contain links to outside resources such as websites or shared network drives.

Content Folios adds the following functionality:

- Organize content into a simple, flat folio structure
- Organize content into an advanced hierarchical folio structure
- Create pre-structured templates for selection when creating folios
- Modify folio structure dynamically
- Lock folio structure to prevent it from being modified dynamically
- Lock content folios to prevent additions
- Unlock folios to allow additions
- Modify folios without tracking revisions
- Take a snapshot of a folio to track revisions
- Download renditions of folio content in `.zip`, `.ppt`, `.pdf`, or XML format

> **Note:**
>
> – Downloading a PDF rendition of a folio having encrypted PDF files throws `classNotfoundexception` on a class that is a part of `bcprov` encryption `jar`. This `jar` along with two others are mentioned as a dependency for the iText 2.1.7 PDF library used by WebCenter Content. See https://mvnrepository.com/artifact/com.lowagie/itext/2.1.7.
>
> – Oracle does not provide an encryption library. The library `bcprov-jdk14-138.jar` is a recommended third-party encryption library that is downloadable from BouncyCastle.org, but any library can be used.

- Create multiple unstructured content baskets for use in collecting content items

Several changes are made to Content Server during installation of Content Folios:

- Additional metadata fields: The following metadata fields are added to record the current state of a folio or template:
  - CpdIsTemplateEnabled
  - CpdIsLocked
- Additional views: The following views are added and are used on the Folio Edit page to communicate Content Folios tables to JavaScript:
  - NodPropertyView
  - LinkPropertyView
  - NodeRemovalTypeView
  - CpdTreeDisplayFunctionMapView
  - CpdPopupEditActionsView
  - ItemPropertyView
  - PneDocProfileView
- Additional Relations: The GenericUserProfileRelation is used by PneDocProfileView.
- Additional Tables: The following tables record the links that folios and content baskets have against content in the system:
  - CpdLinks
  - CpdArchiveLinks
  - CpdBasketLinks
  - CpdEditHistory

Changes made to Content Server remain even if Folios is disabled.

5.3.2 Creating and Using Content Folios

The structure of a folio can be based on a pre-defined template when it is created. The structure can also be modified when creating or editing the folio, as discussed in the following sections:

- Creating and Editing Folio Templates
- Adding Custom Viewers and Renderers

5.3.2.1 Creating and Editing Folio Templates

Folio templates are a predefined organization of nodes, subnodes, slots, and any content items required when creating a folio. The templates are XML files checked in to and are managed by Content Server. A template is selected for use when creating an advanced folio. A template can be edited or revised at any time. Revisions to a template are not applied retroactively to existing folios based on that template, but only apply to new folios created based on the template's new revision.

To create folio templates, you must have administration rights.

To create a folio template:

1. Use the main menu to choose **Administration** then **Folio Administration** then **Create Folio Template**.
2. Save the folio template and check in the folio:
   a. From the page Actions menu, select **Save template**.
   b. Choose the profile to use with the template and click **Next**.
   c. Enter the necessary check-in information, including a descriptive title for the template. Click **Check In**.
3. Add structure or content to the template on the Create/Edit Folio Template page and define the template properties.

   The **Structure** tab of the Create/Edit Folio Template page is divided into three sections:

   - Folio Structure Pane: Shows the nodes, slots, and items that comprise the folio hierarchy. Right click within the folio structure area to display the following options on a contextual menu. Unless noted otherwise, the options are available for nodes, items, and slots:
     - **Insert Selected Source Item**: Inserts a selected item from the Source Items Pane in a slot. If the slot contains an item, it is replaced.
     - **Insert Item by Search**: Opens a search page to find an item to add to the folio in the selected node or slot. If the slot contains an item, it is replaced.
     - **Insert Item by Checkin**: Opens a check-in form used to add an item to be used n the selected node or slot. If the slot contains an item, it is replaced.
     - **Remove Content Item**: Removes content from a slot. It does not remove the slot. (items only)
     - **Insert hypertext**: Creates a new item in the structure that can establish a hypertext link to the specified URL.
     - **Create Node** or **Slot**: Creates a node or slot at the specified location.
     - **Cut, Copy, Paste**: Cuts or copies an item for later pasting if needed.
     - **Delete**: Deletes an item from the structure.
   - Element Info Pane: When a node, slot, or item is selected in the Folio Structure Pane, information about the selection is displayed and optionally modified. Modified information is written back to the XML file that is checked in. Unless noted otherwise, the following fields are available for nodes, items, and slots:

- **Name**: Name of the object.
- **Description**: Description of the object.
- **Attributes** (items and slots): The uses and limitations of the object. Default attributes include the following:

  Allow empty: The object can be left empty.

  Lock content: Items cannot be deleted from the slot.

  Removable: The object can be deleted.

  Allow external: External link can be specified.

  Restrict formats: Limits allowable content item formats through a comma-delimited list that maps formats to file extensions.

  Allow folio: A folio can be specified in the slot.

  Content profile: The content profile used when adding an item by search or check in.

  Clone item: The associated item is cloned. A cloned item is copied and checked in as a new item when a folio based on the template is created. If an item is not cloned, the original content item is associated with any folio created using the template.
- **Attributes** (nodes): Default attributes include the following:

  Removable: The node can be deleted.

  Children movable: Items and slots can be moved within the hierarchy.

  Allow item creation: Items can be created within the node.

  Allow node creation: Subnodes can be created within the node.

  Maximum items, Maximum nodes: Specifies the total number of items allowed in the node.

  Content profile: The content profile used when adding an item by search or check in.
- **Content ID**: (items and slots). The ID of the item.
- **Create Date**: (items and slots). The date a content item was created.
- **Last modified**: (items and slots). The last date changes were made.
- **Link**: (links only): The URL of a link.

- Source Items Pane: Used to collect items to be used in the folio.

4. Click **Finish** when done.

5.3.2.2 Adding Custom Viewers and Renderers

Content Server ships with a default viewer that mimics the structure of the Create/Edit Folios page, and the following rendition options:

- Zip
- PDF
- XML

Custom viewers and renderers can be created, but such development requires an understanding of the following:

- The structure of the folio XML
- The folio Idoc Script functions and their proper usage
- The Iterator/Renderer architecture
- The method for using a component to modify/add to the list of viewers and renderers

To add custom viewers and renderers, contact Oracle Consulting at `http://www.oracle.com/consulting/index.html`.

For information about using a service to return the folio structure as a simple resultset, see the "Crawling a Content Folio" blog.

6
Managing Workflows

Workflows are used to specify how content is routed for review, approval, and release to the system. This chapter provides information for understanding and using the workflow functionality available with Oracle WebCenter Content Server.
This chapter contains the following topics:

6.1 Understanding Workflows

Designing an effective workflow is an iterative process. After initial planning, workflows are refined as the process is implemented. Good planning in the beginning can reduce the amount of rework. For more information on planning, see Planning a Workflow.

Setting up workflows for a business process can provide several advantages:

- Workflows provide good reporting metrics. They can produce an audit trail of who signed off on content at various points of the life cycle of the content.
- Workflows help get the right information to the right person.
- Designing a workflow requires you to examine and understand your business processes, helping you find areas for improvement.

There are three types of workflows:

- A *basic workflow* defines the review process for specific content items, and must be initiated manually.
- A *criteria workflow* is used for content that enters a workflow automatically based on metadata that matches predefined criteria.
- A *sub-workflow* is initiated from a step in another workflow and is created in the same manner as criteria workflows. Sub-workflows are useful for splitting large, complex workflows into manageable pieces.

This section provides details about the functions that make up a workflow:

6.1.1 Workflow Steps

Steps define the process and the functionality of the workflow. Each workflow can include multiple review and notification steps with multiple reviewers to approve or reject the content at each step. For each step in a workflow, a set of users and a step type are defined.

The users defined for a step can perform only the tasks allowed for that step type.

Step Type	Description
Contribution	The initial step of a Basic workflow. Administrators define the contributors when the workflow is created.
Auto-Contribution	The initial step of a Criteria workflow. There are no predefined users involved in this step. The contributor who checks in a content item that enters the workflow process automatically becomes part of the workflow.
Review	Users can approve or reject the content; editing is not allowed. You can also specify that the user must approve and sign the content with an electronic signature.
Review/Edit Revision	Users can edit the content if necessary then approve or reject it, maintaining the revision.
Review/New Revision	Users can edit the content if necessary then approve or reject it, creating a new revision.

> **Note:**
>
> Workflow steps grant a level of access that can override the permissions defined by security roles. For example, a user assigned to a Review/Edit Revisions or Review/New Revision step has the ability to check out and check in items through My Workflow Assignments even if that user has a read-only role to the security group to which those items belong.

After a workflow is enabled, it goes through several specific stages:

- When a content item is approved by the minimum number of reviewers for a particular step, it goes to the next step in the workflow. If the step is defined with 0 approvals required, the reviewers are notified, but the content goes to the next step automatically.
- If any reviewer rejects the content, it goes back to the most recent Review/Edit Revision or Review/New Revision step. If there is no such step, the content goes back to the original author.
- Depending on how the edit criteria is defined, the most recent Review/Edit Revision or Review/New Revision step can result in a new revision or an updated revision.
- A revision can be released:
  - After it exits the workflow: When content is approved at the last step in the workflow, the content item is released to the system.

  - Before it exits the workflow: If a side effect is set that releases a document from edit state, the document is available for indexing, searching, and archiving. Use this primarily for business routing that does not require publishing to the Web, for example an expense report.

- Generally, if a Basic workflow contains multiple content items, none of them are released to the system until all of the items have been released from completion of the workflow. However, if a content item is released from the edit state as a side effect, that content item can be released without waiting for all items in the Basic workflow.

The standard workflow process can be customized to make it more flexible with *jumps, tokens,* and *aliases*. These are discussed fully in Customizing Workflows.

6.1.1.1 Events

Each step in a workflow has three events: entry, update, and exit.

- An *entry* event script is evaluated when entering the step. If the entry event script does not result in a jump or exit, any users, aliases, and tokens are evaluated and email notifications are sent.
- An *update* event script is evaluated at various points (for example, during the hourly update cycle or on check in of the revision). Extra exit conditions are evaluated each time the update event script is evaluated.
- An *exit* event script is evaluated when a revision has completed the step's approval requirements and the step's extra exit conditions are met.

For more information about Jumps, see Jumps and Events.

> **Note:**
>
> Update and exit event scripts are *not* run when a revision is rejected. Any code to be evaluated on rejection must be in the *entry* event script for the step that the rejected content is sent to.

6.1.1.2 Workflow Step Files

The *companion file* is a text file that tracks the steps the revision has been through and maintains the current values of workflow variables. It is only active for the life of the workflow. Each revision in a workflow has a companion file, which exists while the revision remains in the workflow. When a revision is released from a workflow, its companion file is deleted.

Companion files are in HDA file format, and are named by Content ID (for example, `HR_004.hda`). Each companion file contains two sets of data:

- The *LocalData* Properties section defines the Parent List and other workflow variables.
- The *WorkflowActionHistory* ResultSet section contains a record of the steps, workflow actions, and users that have been involved in the revision's workflow history.

To retain a companion file, add the `IsSaveWfCompanionFile` configuration variable to the `/config/config.cfg` file and set the parameter to true. For more information, see the *Configuration Reference for Oracle WebCenter Content*.

The companion file uses *keys* to keep track of workflow variables. For example, the following keys define the value of the `EntryCount` and `Last Entry` variables for an Editor step in a workflow called `Marketing Brochures`:

```
Editor@Marketing Brochures.entryCount=1
Editor@Marketing Brochures.lastEntryTs={ts '2001-05-02 16:57:00'}
```

The companion file maintains a *parent list*, which lists the sequence of steps that the revision has been through, starting with the current step and working backward. The parent list is used to determine which step to return to when a file is rejected, when the last step of a workflow is finished, or when an error occurs. For example, the following parent list shows the *Marketing Team*, *Editor*, and *Graphic Artist* steps of the *Marketing Brochures* workflow:

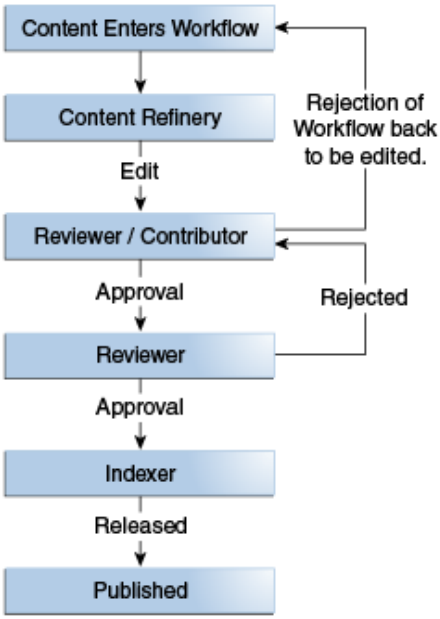
```
WfParentList=Marketing Team@Marketing Brochures#Editor@Marketing
Brochures#Graphic Artist@Marketing Brochures#contribution@Marketing Brochures
```

An asterisk (*) in front of a step name in the parent list indicates a jump step.

6.1.2 Workflow Evaluation Process

Figure 6-1 shows a general workflow process.

Figure 6-1 Workflow Process



When a revision enters a workflow step:

1. The entry script is evaluated.
   - The default entry script that keeps track of the entry count and last entry is updated.
   - Actions (such as additional user notification) are executed.
   - If the jump condition is met and a target step is defined, the revision jumps to another step.

- If the jump condition is not met, reviewers for the current step are notified that the revision is ready for approval.
- To avoid infinite loops, the entry script of a previously visited step is ignored. The only exception is when the step has been restarted using the `wfCurrentStep(0)` symbolic step.

2. When the required number of reviewers have approved the revision, the exit script is evaluated.
   - If there is no exit script, the revision goes to the next step in the workflow.
   - If an exit script jump condition is met and a target step is defined, the revision jumps to another step.
3. After the exit script is evaluated, the current action state (the `wfAction` workflow variable) is set. The following are the possible actions:
   - APPROVE
   - REJECT
   - CHECKIN
   - CONVERSION
   - META_UPDATE
   - TIMED_UPDATE
   - RESUBMIT
4. As a revision moves through the steps of a workflow, each step is added to the parent list. If the revision revisits a step, the parent list returns to the state it was in when the revision first visited that step. For example:

Revision goes to:	Parent list
Step1	Step1
Step2	Step1#Step2
Step3	Step1#Step2#Step3
Step2	Step1#Step2

5. If a revision is rejected, the parent list is checked for the most recent Reviewer/ Contributor step, and the revision goes to that step in the workflow.
6. When a revision completes the last step in a workflow, the parent list is checked for the most recent jump step with a defined return step. If a return step is found, the revision goes to that step. If there are no jump steps in the parent list, or none of the jump steps have a return step defined, the revision exits the workflow.

Content items in a workflow can have the following statuses.

Status	Criteria Workflow	Basic Workflow
EDIT	The content item was rejected and returned to the initial contribution step.	The content item is in the initial contribution step, or the content item was rejected and returned.
REVIEW	The content item is in the review process.	The content item is in the review process.

Status	Criteria Workflow	Basic Workflow
PENDING	N/A	The content item completed all the workflow steps, but other content items in the workflow (if included) are not finished.
DONE	The content item in the workflow is finished.	All of the content items are finished.
GENWWW	The content is being converted to Web-viewable format.	The content is being converted to Web-viewable format.
RELEASED	The revision is available in Content Server.	The revision is available in Content Server.

6.1.3 Workflow Participation

Email is sent to the participating contributors in a Basic workflow who must check in designated content. Email is also sent to reviewers involved in workflow steps. Users can check their necessary actions on the Workflow Content Items page. To access the Workflow Content Items page, use the main menu to choose **Content Management** then **Active Workflows**.

Reviewers can review content, reject or approve content, and view information about the content and the workflow. If the content is rejected, the Reject Content Item page opens where the reviewer can enter a message to explain the reason for rejection. The message is sent to the reviewers assigned to the last step allowing a contribution. Those reviewers can then check out the content, edit it and check the content back in. On the Content Check In form, the reviewer should select the Revision Finished Editing box. The content then goes to the next step in the workflow. If the box is not selected, the content remains in Review status and must be approved before moving on through the workflow.

It is good practice to discuss workflows with the people involved so they are aware of the responsibilities they have in the process. More information about workflow participation is available in *Using Oracle WebCenter Content*.

6.2 Planning a Workflow

This section describes the steps to follow to choose a workflow type and plan the workflow:

- Choosing a Workflow Type
- Designing a Workflow
- Modifying Workflows

Before beginning to design a workflow, evaluate how processes currently operate. For example, if you use email loops to manage information between users on a project, can you incorporate that type of scenario into a workflow design?

Is the workflow being used to validate information? Or is it used for collaboration? What specific problem is it addressing? After you understand the current processes and their shortcomings, you can design the workflow to solve the problem.

Ask the following questions when designing a workflow:

- Who is involved in the workflow? What users receive notification when an item is ready for review? Who has edit permissions? Who has final sign-off?

  Equally important is to ask who is left out of a workflow.

  How do you train the people who are involved in the workflow?
- What happens when an item is in the workflow? What action is taken when an item is approved, rejected, or updated? What should occur when an item stays in a workflow too long?
- When must an item be moved to the next stage of a workflow? What is the criteria for determining when a workflow is completed?
- Where do users go to participate in a workflow? Is there a Web interface?
- How are approvals and rejections handled? Will audit information be stored? Are electronic signatures required?

6.2.1 Choosing a Workflow Type

Use a **Basic Workflow** when you must:

- Specify an 'ad hoc' workflow, one that does not depend on specific criteria to be enabled.
- Route multiple content items to go through the same series of steps. The items go through the steps individually, but are not released until all items are finished in the workflow.
- Notify or remind a user to contribute a content item to the workflow.
- Specify a workflow that is used infrequently.
- Set up the review process for a group of related content items.
- Specify a user to start the workflow. Content can enter a Basic workflow only when a user with Workflow rights starts the workflow.

Use a **Criteria Workflow** when you must:

- Have content enter a workflow automatically based on specific metadata values.
- Route single content items that match specific criteria. Multiple items can be routed, but they do not progress through the workflow as a unit.
- Set up a standardized review process for individual documents.
- Specify a frequently-used workflow.
- Open the workflow to many users. Users do not need Workflow rights for their content to enter a Criteria workflow.

When deciding which type of workflow to use, keep the following key points in mind:

- If content is checked in with the wrong security group or wrong metadata value, it can enter a Criteria Workflow accidentally.
- If users are frequently processing content through the same Basic workflow, consider setting up a Criteria workflow to automate the process.
- Do not use the same or overlapping criteria for multiple workflows. If a content item matches the criteria for multiple workflows, it enters the first workflow in the list.
- When a content item is in a criteria workflow, it cannot be deleted until the item is released.

6.2.1.1 Security Issues

Keep the following security issues in mind when administering workflows:

- Each workflow is associated with a security group.
  - For a Criteria workflow, only content items in the same security group enter the workflow.
  - For a Basic workflow, new content items are assigned to the security group of the workflow, and existing content items must belong to the workflow's security group.
- A workflow can only jump to another workflow in the same security group.
- The security group of a workflow cannot be changed while a workflow is active but the security group of an item in the workflow process can be changed.
- Workflow rights and admin permission for the security group of the content are needed to set up a workflow and start it.
- Workflow templates can be used to initiate contribution steps.
- Write permission to the workflow's security group is required to be a contributor to the workflow.

6.2.2 Designing a Workflow

To design a workflow:

1. Draw a flowchart of the workflow. For examples, see Criteria Workflow Process and Basic Workflow Process.
2. Verify all the metadata needed for the workflow. If needed, create the metadata before setting up the workflow.
3. Set up the aliases for the workflow. Alias creation is discussed in *Administering Oracle WebCenter Content*.
4. Set up the tokens for the workflow. For more information, see Creating, Editing, or Deleting a Token.
5. Set up a Basic or Criteria workflow. If workflow templates are available, consider using a template as a starting point. For more information, see Workflow and Script Templates.
6. Set up sub-workflows if necessary.
7. Set up jumps. For more information, see Creating a Jump.
   - If script templates are available, use them to create the step event scripts.
   - If jumps are used, consider setting up a "master" workflow with sub-workflows for each jump.
8. Test the workflow.
   - For a Criteria workflow, check in a test document that matches the defined security group and metadata field value.
   - For a Basic workflow, define test content and start the workflow.
   - Simulate as many approval/rejection scenarios as possible.

- For workflows that contain jumps, simulate as many event scenarios as possible.
- Include reviewers in the workflow testing to verify that people understand their roles.

6.2.3 Modifying Workflows

Keep these points in mind during workflow design:

You can:

- Modify the criteria for a Criteria workflow.
- Add or delete content items from a Basic workflow.
- Modify step definitions (including reviewers, exit conditions, and events)

You cannot:

- Change the order of the steps. You can delete steps and re-create them in new locations.
- Add steps in the middle of the workflow. New steps are always added to the end of the workflow.
- Delete a content item while it is in a criteria workflow.
- Archive content items that are in either a basic or criteria workflow.

If you disable a Criteria workflow or cancel a Basic workflow to add or delete steps, any revisions in the workflow are released (Criteria workflow) or deleted (Basic workflow).

The following tips can help when modifying existing workflows. Altering a workflow in use is a time-consuming and difficult process. Careful design before implementation can help avoid rework. These options are considered a temporary correction until the workflow can be rebuilt.

- Consider the following options to reorder steps in an existing workflow:
  - Create a sub-workflow and add a jump to it from an existing step. This change can be made to an existing step without disabling or canceling the workflow.
  - Add step event scripts to an existing step to define the actions that would normally take place in a separate step. This change can be made to an existing step without disabling or canceling the workflow.
- If a workflow must be disabled to modify it (for example, to add a step) all revisions are immediately released from the workflow (Criteria workflow) or deleted (Basic workflow). To disable a workflow without releasing content:
  1. Clone the workflow to a static workflow which has the same step sequence as the original workflow but which has no step logic. The content goes into a step and stays there until moved.
  2. Create an update event in the original workflow. This event is triggered by time and pushes the content into the cloned static workflow at the appropriate step.
  3. When the content is out of the original workflow, disable the workflow, make the necessary changes, then re-enable it. Then use the same timed event logic to move the content from the cloned workflow back to the original workflow.

6.3 Creating a Criteria Workflow

Criteria workflows are used to set up a review process for individual documents that enter the workflow automatically when they match predefined criteria. For example, any time a new purchase order is generated, it might be automatically routed to specific reviewers for approval.

A Criteria workflow includes the following:

- Criteria defined by a security group and one metadata field.
- Auto-contribution step with no predefined users.
- One or more reviewer steps with one or more reviewers per step.

Sub-workflows are set up using the same procedure as Criteria workflows with a few minor exceptions which are noted in the procedure for setting up Criteria workflows.

This section discusses the following topics:

6.3.1 Criteria Workflow Process

The following steps briefly explain the Criteria workflow process:

1. A user with Workflow rights sets up the Criteria workflow by defining the following:
   - Security group
   - Metadata field and value (for example, *ContentType matches PurchaseOrder*). You can use fields of type Text or Long Text.
   - Review steps and reviewers for each step
   - The number of approvals required for each step. For example, must all reviewers approve it before it can move to the next step?
   - Any aliases and the people in the alias group
   - Any tokens needed
2. A user with Workflow rights enables the Criteria workflow.
3. When content is checked in that matches the defined security group and metadata field value, the content enters the workflow.
4. Reviewers for the first step receive email that the revision is ready for review.
5. The reviewers approve or reject the revision.
   - If the step is a reviewer step, the reviewers can optionally sign and approve the content item revision without modification (changing the document produces a different identifier and invalidates any existing electronic signatures).

- If the step is a reviewer/contributor step, the reviewers can check out the revision, edit it, and check it back in before approving it. For example, editors can alter the content of an item in the workflow.
- If a user rejects the revision, the workflow returns to the previous contribution step, and the users for that step are notified by email.
- When the minimum number of users have approved the revision, it goes to next step. If the minimum number of approvals is 0, the revision moves to the next step automatically.

6. When all steps are complete, the revision is released to the system.

6.3.1.1 Criteria Workflow Tips

Each Criteria workflow must have unique criteria. If a content item matches the criteria for two workflows, it enters the first one in the list of defined workflows.

- All users assigned to the Criteria workflow must have Read permission to the selected security group. Contributors must have Write permission to the selected security group to check the revision in and out.
- You cannot add or delete steps while a Criteria workflow is enabled.
- You cannot delete or archive a content item while it is in a criteria workflow.
- Any content item checked in while a Criteria workflow is disabled bypasses the workflow process and is released to the system.
- Disabling a Criteria workflow releases revisions in the workflow to the system.
- A Criteria workflow can use jumps to sub-workflows and other Criteria workflows in the same security group, and can jump to other steps in the same workflow.
- Consider making at least one step in the workflow a Reviewer/Contributor step so rejected revisions go to that step rather than back to the original author.
- If the security group of an item does not match the security group of the workflow, the item does not enter the workflow.
- Ensure that the criteria is different from other Criteria workflow.
- If Content ID is used for the Field and if an Oracle database is used, enter all uppercase characters for the Value. All other fields can have mixed case.
- If ContentID is used as the Field, click **Select** below the Value field to choose an existing content item.
- Enter zero (0) in the **At least this many reviewers** field to notify reviewers that the revision has reached the step and to pass it on to the next step automatically. Reviewers cannot approve, reject, or edit the revision at that step.

6.3.2 Setting Up a Criteria Workflow

To create a Criteria workflow or sub-workflow:

1. Use the main menu to choose **Administration** then **Admin Applets**.
2. Click **Workflow Admin** then click the **Criteria** tab.
3. Click **Add**.

4. On the New/Edit Criteria Workflow page, enter a name in the **Workflow Name** field. Maximum length is 30 characters. Special characters (; @&, and so on) are not allowed. You cannot change the workflow name after the workflow is created.
5. Enter a detailed description for the workflow in the **Description** field.
6. Select the Security Group from the list.
7. Select an option from **Original Author Edit Rule** to specify if the original author can edit the revision or create a new revision if the item is rejected.
8. To use a workflow template, select the **Use Template** check box and select the template name. This box is displayed only if a template currently exists. For more information, see Workflow and Script Templates.
9. To create a Criteria workflow, select the **Has Criteria Definition** check box. To create a sub-workflow, deselect the check box.
10. For a Criteria workflow, define the criteria by choosing the appropriate **Field**, **Operator**, and **Value**. Field values include Content ID, Author, Type, Account and any custom metadata of type Text or Long Text.
11. Click **OK**.
12. If a template was not used to create steps or to add another step, click **Add** in the right pane of the Workflow Admin page.
13. On the Add New/Edit Step page, enter an appropriate **Name** for the step. You cannot change the name after the step is created. The name is usually descriptive of the step (for example, *EditorialReview* or *TechnicalReview*).
14. To require that a reviewer provide credentials for an electronic signature, select **Requires signature on approval**. This option is available only if the Electronic Signatures component is enabled.

    An electronic signature uniquely identifies the contents of the file at a particular revision and associates the signature with a particular reviewer. If selected, the standard **Approve** action is replaced by the **Sign and Approve** action in the list of step options provided to the reviewer.
15. Enter a **Description** for the step.
16. Specify the authority level of the users for the step:
    - Users can review the current revision: Users can approve or reject the revision but cannot edit the revision.
    - Users can review and edit (replace) the current revision: Users can edit the revision, approve it, or reject it. An edit does not update the revision.
    - Users can review the current revision or create a new revision: Users can edit the revision, approve it, or reject it. An edit updates the revision. This option preserves the original content and provides an audit trail of changes.
17. Select the type of users to be added to the step. Multiple types can be defined:
    - To add a group of users defined by an alias, click **Add Alias**. On the Add Alias to Step page, choose the alias from the displayed list.
    - To add individual user logins, click **Add User**. On the Add User to Step page:
      – To narrow the list of users, select the **Use Filter** check box, click **Define Filter**, select the filter criteria, and click **OK**.
      – To select a range of users, click the first user, then press and hold Shift and click the last user in the range.

  - To select users individually, press and hold the Ctrl key and click each user name.
- To add a variable user defined by a token, click **Add Token**. For information about creating tokens, see Creating, Editing, or Deleting a Token.

18. Click **OK**.
19. Click the **Exit Conditions** tab.
20. Specify how many reviewers must approve the revision before it passes to the next step.
    - To require approval by all reviewers, select **All reviewers**.
    - To specify a minimum number of reviewers who must approve the revision, select **At least this many reviewers** and enter the number.
21. Typically, exit conditions are useful when metadata could be changed by an external process during the workflow step. Use the following instructions if the step requires additional exit conditions to pass to the next step:
    a. Select the **Use Additional Exit Condition** check box.
    b. Click **Edit**.
    c. On the Edit Additional Exit Condition page, select a workflow condition or a metadata field from the **Field** list.
    d. Select an operator from the **Operator** list. **Operator** is a dependent choice list that shows operators associated with the Field.
    e. Select a value from the **Value** list. **Value** is a dependent list based on the option chosen as the Field.
    f. Click **Add** to add the conditional statement to the Condition Clause. The clause appears in the Condition Clause box. You can append multiple clauses with `AND` statements.
    g. Repeat for as many conditions as required. To modify an expression, select it in the Condition Clause box, change the Field, Operator, or Value, and click **Update**.
    h. To modify the condition expression, select the **Custom Condition Expression** check box and edit the script (for example, use `OR` not `AND` for a condition). The additional exit conditions must be Idoc Script statements that evaluate to true or false. Do not enclose the code in Idoc Script tags <$ $>.

    > **Caution:**
    >
    > If **Custom Condition Expression** is deselected, the expression reverts to its original definition and all modifications are lost.

    i. Click **OK**.
22. If the workflow requires conditional steps or special processing, click the **Events** tab and add the appropriate scripts. For more information, see Creating a Jump.
23. Click **OK**.
24. Add, edit, and delete steps as necessary to complete the workflow.
    - To add another step to the workflow, repeat steps 12 through 23.
    - To edit an existing step, select the step and click **Edit**.

- To delete an existing step, select the step and click **Delete**.

25. Ensure that the correct workflow is selected in the left pane, and click **Enable**.
26. On the confirmation page, click **Yes** to activate the selected workflow.

6.3.3 Changing a Criteria Workflow or Sub-Workflow

If a Criteria workflow is disabled to add or delete steps, any revisions in the workflow are released.

To change an existing Criteria workflow or sub-workflow:

1. Use the main menu to choose **Administration** then **Admin Applets**.
2. Click **Workflow Admin** then click the **Criteria** tab.
3. Select the workflow to change in the left pane.
4. To add or delete steps, click **Disable**.
5. Click **Add, Edit,** and **Delete** in the left and right panes to change the following:
   - workflow description
   - security group
   - type of workflow (Criteria or sub-workflow)
   - criteria
   - step description
   - type of step (reviewer, contributor same revision, contributor new revision)
   - users
   - events
   - number of approvals required
   - exit conditions

   Users can be added to a step while the Criteria workflow is enabled, but if any revisions are currently at that step in the workflow, the new users are not notified immediately. They are notified after the scheduled workflow system event occurs and performs a `TIMED_UPDATE` on all items in the workflow.
6. If the workflow is disabled, ensure that the correct workflow is selected in the left pane and click **Enable**.
7. On the confirmation page, click **Yes** to activate the selected workflow.

6.3.4 Disabling a Criteria Workflow or Sub-Workflow

To disable a criteria workflow or sub-workflow:

1. Use the main menu to choose **Administration** then **Admin Applets**.
2. Click **Workflow Admin**, then click the **Criteria** tab
3. Select the workflow.
4. Click **Disable**.
5. If any content items are still in the workflow process, you are notified that all of the content revisions will be released. If you do not want to release the content, click

No to cancel the operation. Click **Yes** to release any content and disable the workflow.

The status of the workflow changes to **Disabled**.

6.4 Creating a Basic Workflow

A Basic workflow defines the review process for specific content items. It is set up and initiated manually, and does not require you to define criteria for content to enter the workflow.

A Basic workflow includes the following:

- One or more content items.
- Initial contribution step with one or more contributors.
- Zero or more review steps with zero or more reviewers per step.

This section discusses the following topics:

6.4.1 Basic Workflow Process

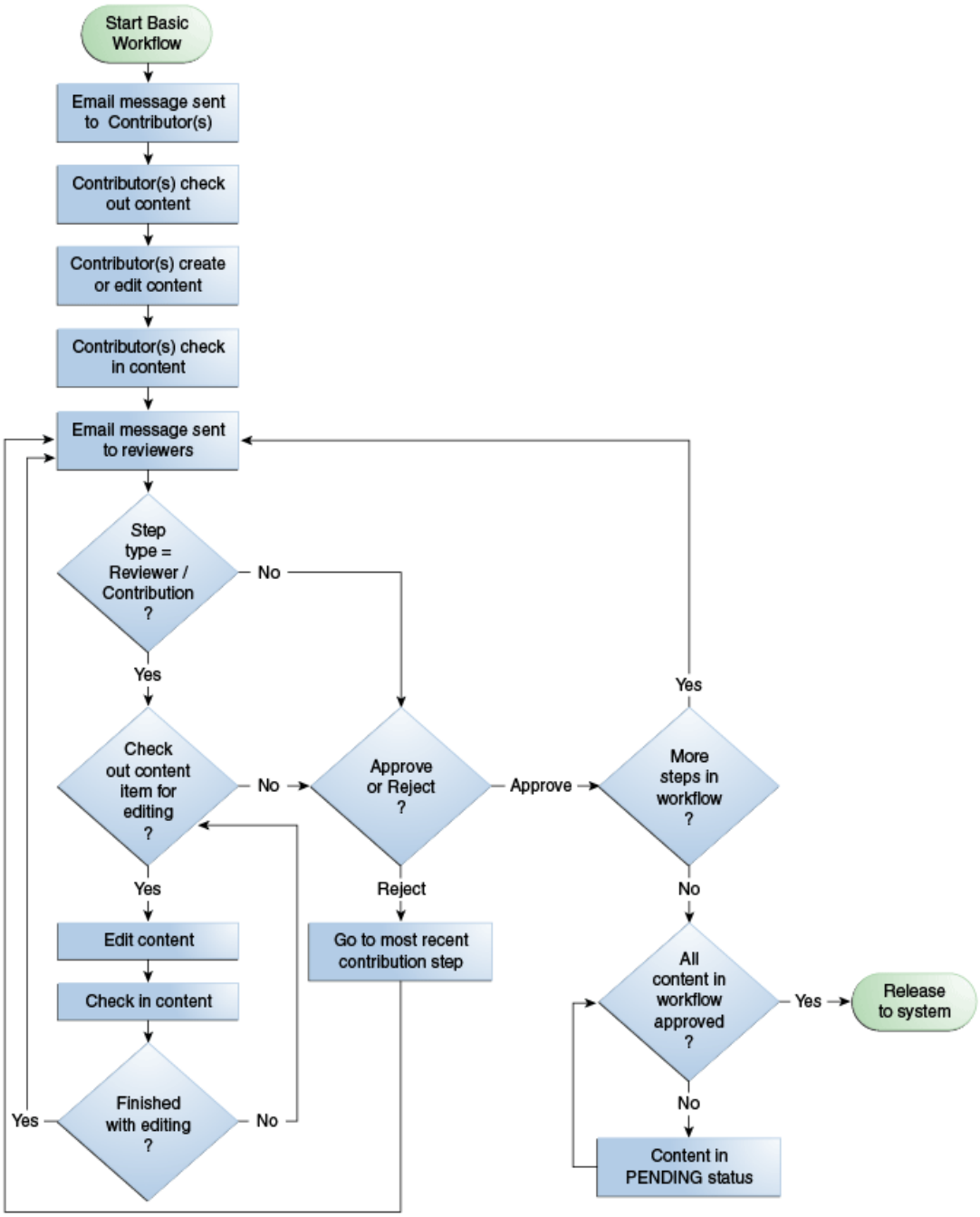
The following steps explain the Basic workflow process:

1. A user with Workflow rights sets up the Basic workflow by defining the following items:
   - Content: Either create new content or select existing content. After going through the workflow, new content is released to the system at revision 1, and existing content is released to the system at the next revision number for that content item.
   - Initial contributors: Specify the list of user who can contribute content.
   - Review steps: Specify the reviewers for each step and number of approvals required for each step.
2. A user with Workflow rights starts the Basic workflow by enabling it.
3. An email is sent to the contributors.
4. Any of the contributors can check out then check in a file for each content item in the workflow.
5. Reviewers for the first step are notified by email that the revisions are ready for review.
6. The reviewers approve or reject the revisions.
   - If the step permits editing, the reviewers can check out the revisions, edit them, and check them back in before approving it.
   - If a user rejects a revision, the revision returns to the previous contribution step, and the users for that step are notified by email.
   - When the minimum number of users have approved the revision, it goes to next step. (If the minimum number of approvals is 0, the revision moves to the next step automatically.)
7. Generally, if a Basic workflow contains multiple files, none of them are released to the system until all of the files have been released from completion of the workflow.

Completed content items stay in PENDING status until the last revision is approved. However, if you release a content item from the edit state as a side effect, you can release that content item without waiting for all items in the Basic workflow.

8. When all steps are complete and all revisions are approved, the revisions are released to the system.

Figure 6-2 Basic Workflow Process



6.4.2 Basic Workflow Tips

- For new content, the Content ID defined in the workflow is the Content ID applied when the revision is released to the system. The Content ID cannot be changed.
- A content item cannot be added to multiple basic workflows or an error occurs and the workflow is not enabled.
- New content is assigned to the security group of the Basic workflow.
- The security group of an existing revision must match the security group of the Basic workflow.
- All users assigned to the Basic workflow must have Read permission to the selected security group. Contributors must have Write permission to the selected security group to edit revisions.
- Review steps cannot be added, edited or deleted while a Basic workflow is active.
- If an active workflow is canceled, any revisions in the workflow are deleted from the system. Any edits made to the files are lost unless they have also been saved on a local hard drive.
- An inactive Basic workflow can be reused, but it must be started manually each time.
- A Basic workflow can use jumps, but only to other steps in the same workflow. A Basic workflow cannot jump to a sub-workflow.

6.4.3 Setting Up a Basic Workflow

Keep these points in mind before creating a Basic workflow:

- All users assigned to the workflow must have Read permission to the selected security group, and Contributors must have Write permission.
- If using a template, change the reviewers if they are different from those defined in the selected template.
- Do not add a content item to multiple basic workflows or an error occurs and the workflow is not enabled.
- Enter zero (0) in the **At least this many reviewers** field to notify reviewers that the revision has reached the step. Reviewers cannot approve, reject, or edit the revision at that step. The workflow passes to the next step automatically.

To create a Basic workflow:

1. Display the **Workflow Admin: Workflows** tab. The default tab view is that of a Basic workflow.
2. Click **Add**.
3. On the Add New/Edit Workflow page, enter a name in the **Workflow Name** field. The Workflow Name has a maximum field length of 30 characters and cannot contain special characters (; @&, and so on). The name cannot be changed after the workflow is created.
4. Enter a detailed description for the workflow in the **Description** field.
5. Select the Security Group from the list to which the content items in this workflow belong.

6. Select an option from **Original Author Edit Rule** to specify if the original author can edit the existing revision or create a new revision if the content item is rejected.
7. To use a template, select the **Use Template** check box and select the template name. This box is displayed only if a template exists. For more information, see Workflow and Script Templates.
8. Click **OK**.
9. To add a new content item to the workflow, click **New**.

   On the Add Content to Workflow (New Content) page:

   a. Enter a Content ID for the new content item. The Content ID cannot be changed. To change a Content ID, delete the content item from the list and re-add it. If using an Oracle database, all Content IDs are converted automatically to uppercase letters.

   b. Click **OK**.
10. To add an existing content item to the workflow, click **Select**.

    On the Add Content to Workflow (Existing Content) page:

    - To narrow the list of content items, specify criteria for the filter, release date or both.
    - To select a range of content items, click the first content item, then press and hold **Shift** and click the last content item in the range.
    - To select content items individually, press and hold the Ctrl key and click each content item.

    Existing content items must have the same security group as the workflow.
11. Repeat steps 9 and 10 as necessary to add content items to the workflow.
12. Define one or more contributors for the initial contribution step. You can define multiple types of users for the contribution step.
    - To add a group of users defined by an alias, click **Add Alias** to open the Add Alias to Workflow page.
    - To add individual user logins, click **Add User** to open the Add User: Basic Workflow page.
      – To narrow the list of users, select the **Use Filter** check box, click **Define Filter**, select the filter criteria, and click **OK**.
      – To select a range of users, click the first user, then press and hold **Shift** and click the last user in the range.
      – To select users individually, press and hold the Ctrl key and click each user name.
13. If a template was not used to create review steps, or to add another step, click **Add** in the right pane near the Steps box.
14. On the Add New/Edit Step page, enter an appropriate **Name** for the step. You cannot change the name after the step is created. The name is usually descriptive of the step (for example, *EditorialReview* or *TechnicalReview*).
15. To require that a reviewer provide credentials for an electronic signature, select **Requires signature on approval**. This option is available only if you enabled the Electronic Signatures component.

An electronic signature uniquely identifies the contents of the file at a particular revision and associates the signature with a particular reviewer. If you select this option, the standard **Approve** action is replaced by the **Sign and Approve** action in the list of step options provided to the reviewer.

16. Enter a **Description** for the step.
17. Specify the authority level of the users for the step.
    - Users can review the current revision: Users can approve or reject the revision.
    - Users can review and edit (replace) the current revision: Users can edit the revision, approve it, or reject it. Any edit does not update the revision of the content item.
    - Users can review the current revision or create new revision: Users can edit the revision, approve it, or reject it. Any edit updates the revision of the content item which preserves the original content and provides an audit trail of changes.
18. Select the type of users to be added to the step. Multiple types of user can be defined:
    - To add a group of users defined by an alias, click **Add Alias** to open the Add Alias to Step page.
    - To add individual user logins, click **Add User** to open the Add User: Basic Workflow page. To narrow the list use the **Use Filter** check box; to select a range of users, click the first user, then press and hold **Shift** and click the last user name in the range. To select users individually, press and hold the Ctrl key and click each user name.
    - To add a variable user defined by a token, click **Add Token**. For more information, see Creating, Editing, or Deleting a Token.
    - Click the **Exit Conditions** tab.
    - Specify how many reviewers must approve the revision before it passes to the next step.
    - To require approval by all reviewers, select **All reviewers**.
    - To specify a minimum number of reviewers who must approve the revision, select **At least this many reviewers** and enter the number.
19. Typically, exit conditions are useful when metadata could be changed by an external process during the workflow step. Use the following instructions if the step requires additional exit conditions to pass to the next step:
    a. Select the **Use Additional Exit Condition** check box.
    b. Click **Edit**.
    c. On the Edit Additional Exit Condition page, select additional criteria from lists.
    d. Select a workflow condition or a metadata field from the **Field** list.
    e. Select an operator from the **Operator** list. **Operator** is a dependent list that shows operators associated with the Field.
    f. Select a value from the **Value** list. **Value** is a dependent list based on the option chosen as the Field.
    g. Click **Add** to add the conditional statement to the Condition Clause. The clause appears in the Condition Clause box. You can append multiple clauses with `AND` statements.
    h. Repeat for as many conditions as required. To modify an expression, select it in the Condition Clause box, change the Field, Operator, or Value, and click **Update**.

i. To modify the condition expression, select the **Custom Condition Expression** check box and edit the script (for example, use `OR` not `AND` for a condition). The additional exit conditions must be Idoc Script statements that evaluate to true or false. Do not enclose the code in Idoc Script tags `<$ $>`.

> **Caution:**
>
> If **Custom Condition Expression** is deselected, the expression reverts to its original definition; all modifications are lost.

j. Click **OK**.

20. If the workflow requires conditional steps or special processing, click the **Events** tab and add the appropriate scripts. For more information, see Creating a Jump.
21. Click **OK**.
22. Add, edit, and delete steps as necessary to complete the workflow.
    - To add another user to the initial contribution step, repeat step 12.
    - To delete a user from the initial contribution step, click **Delete**.
    - To add another review step to the workflow, repeat steps 13 through 21.
    - To edit an existing review step, select the step and click **Edit**.
    - To delete an existing review step, select the step and click **Delete**.
23. Ensure that the correct workflow is selected in the left pane, and click **Start**.
24. On the Start Workflow page, enter a message to be sent to the contributors.
25. Click **OK**.

6.4.4 Changing a Basic Workflow

To change an existing Basic workflow:

1. Display the **Workflow Admin: Workflows** tab.
2. Select the workflow to change in the left pane.
3. To change the workflow security group or the number of review steps in an active workflow, first click **Cancel** to cancel the workflow.
4. Click **Edit** in the left pane to change the workflow description or the security group.
5. Click **New** then **Select** then **Delete** in the Content pane to add or delete content from the workflow.
6. Click **Add Alias** then **Add User** then **Delete** in the Contributors pane to add or delete contributors from the initial contribution step.

> **Caution:**
>
> Content items can be changed in a Basic workflow after it has started, but the contributors are not notified automatically. Contributors can be changed after the workflow is started, but any new contributors are not notified immediately.

7. Click **Add** then **Edit** then **Delete** in the Steps pane to change the following:
   - Requires signature on approval (optional Electronic Signatures option)
   - Step description
   - Type of step (reviewer or reviewer/contributor)
   - Users
   - Events
   - Number of approvals required
   - Exit conditions

6.5 Customizing Workflows

Tokens and jumps are used to customize workflows to accommodate different business scenarios. A *token* defines variable users in a workflow and a *jump* branches a workflow to a different side effect.

This section describes how to set up and use tokens and jumps. It discusses the following topics:

- Idoc Script Functions and Variables
- Workflow Tokens
- Workflow Jumps

6.5.1 Idoc Script Functions and Variables

Jumps and tokens are created using Idoc Script. The interfaces create the correct syntax and usage for you when you create tokens and jumps. However, you can customize your scripts using the following Idoc Script functions. For more information about usage, see *Developing with Oracle WebCenter Content*.

Idoc Script Functions

Function	Description
wfAdditionalExitCondition	Retrieves the exit condition defined for the current step.
wfAddUser	Adds a user, alias, or workflow token to the list of reviewers for a workflow. Use this function only inside a token.
wfCurrentGet	Retrieves a local state value from the companion file.
wfCurrentSet	Sets the local state value of a key in the companion file.
wfCurrentStep	Retrieves the name of a step relative to the current step.
wfDisplayCondition	Retrieves the exit condition for a workflow step.

Function	Description
wfExit	Exits a workflow step. Can be used to exit the workflow.
wfGet	Retrieves a state value from the companion file.
wfGetStepTypeLabel	Takes an internal workflow step value and turns it into a human-readable label.
wfIsReleasable	Indicates if the document is released (as far as the workflow is concerned).
wfJumpMessage	Defines a message to be included in the notification email that is issued when a jump is entered.
wfLoadDesign	Used to retrieve information about the existing steps in a workflow or about the exit conditions in a workflow.
wfNotify	Sends an email to a specified user, alias, or workflow token.
wfReleaseDocument	Causes a workflow to release all outstanding document revisions for a document currently being locked by the workflow.
wfSet	Sets a key with a particular value in the companion file.
wfUpdateMetaData	Defines a metadata value for the current content item revision in a workflow.

Idoc Script Variables

Variable	Description
wfAction	The action currently being performed on the revision.
wfJumpEntryNotifyOff	Turns on/off the jump notification.
wfJumpName	The name of the current jump.
wfJumpReturnStep	The name of the step in the parent workflow that the revision returns to when exiting a workflow after the current jump.
wfJumpTargetStep	The name of the step where the revision jumps if the conditions are met.
wfMailSubject	Defines the subject line of a workflow email notification.
wfMessage	Defines a message to be included in a workflow email notification. HTML tags are not supported.
wfParentList	List of the workflow steps that the revision has visited.
wfStart	Sends the revision to the first step in the current workflow.

6.5.2 Workflow Tokens

Use a token for the following purposes:

- Add a variable to a workflow which is interpreted to be a specific user or class of user when the workflow is run.
- Include users and aliases in workflow jumps.
- Define users with conditional statements.

A token assignment is unique and local to each document in a workflow. The logic used to assign the token of one document does not affect other documents in the workflow.

Several sample workflow tokens are included which can be used as-is, or can be modified.

> **Important:**
>
> If a token does not resolve to any valid user names, the token is ignored. If no valid users are defined for a step, the revision moves to the next step in the workflow. For this reason, it is a good idea to identify at least one defined user for each step.

This section discusses the following information about tokens:

- Token Syntax
- Creating, Editing, or Deleting a Token
- Token Examples

6.5.2.1 Token Syntax

The Idoc Script function for tokens, `wfAddUser`, takes two parameters:

- User: The metadata field, alias name, or a variable that resolves to a user name or alias.
- Type: The type of token, either user or alias.

All Idoc Script commands begin with <$ and end with $> delimiters. For example:

```
<$wfAddUser(dDocAuthor, "user")$>
<$wfAddUser("MktTeam", "alias")$>
<$wfAddUser("myUserList", "alias")$>
```

For more information about Idoc Script syntax and usage, see *Developing with Oracle WebCenter Content*.

6.5.2.2 Creating, Editing, or Deleting a Token

To create a token to represent one or more unspecified users, such as the document author:

1. Use the main menu to choose **Administration** then **Admin Applets**.
2. Click **Workflow Administration**.
3. Choose **Tokens** from the **Options** menu.
4. On the Workflow Tokens page, click **Add**.
5. On the Add/Edit Token page, enter a token name in the **Token Name** field. You cannot change the **Token Name** after you create the token. Try to use a descriptive name for the token (for example, *GetOriginalAuthor*, or *AuthorManager*).
6. Enter a detailed description in the **Description** field.
7. Click **Add**.
8. On the Add Token User page, select **User** or **Alias**.
9. Enter a metadata field that will resolve to a user or alias.
   - To specify the original author of the content item, enter **dDocAuthor**.
   - To specify an alias, type the alias name. See the **Screen Aliases** tab on the User Admin page for a list of defined aliases.

10. Click **OK**. The Idoc Script containing the value you specified is shown in the User window.
11. Repeat steps 7 through 10 to add another user or alias.
12. To create a conditional token, edit the Users field. For an example, see Token Examples.
13. Click **OK**.

To change an existing workflow token, follow the previous steps and select the token to change. Click **Edit**. Make any necessary changes and click **OK**.

To delete a token, select the token from the list and click **Delete**.

6.5.2.3 Token Examples

The following examples illustrate how to use tokens in workflows.

Example 6-1 Original Author the Only Contributor

This example assumes that the original author is the only contributor for the file. Example 6-2 addresses the situation where different authors could check out and check in the file during the workflow process.

To notify the original author of each file when their content is released from a workflow into the system, first create a token that corresponds to the **Author** metadata field, which is called `dDocAuthor` in Idoc Script. When setting up the workflow, create a notification step (0 approvals required) and select the token as the user for that step. For example:

```
<$wfAddUser(dDocAuthor, "user")$>
```

Example 6-2 Workflow with Reviewer/Contributor Steps

If a workflow includes Reviewer/Contributor steps, a user other than the original contributor could check in a revised file, and the `dDocAuthor` would no longer be the original author. In this case, you could set the `OriginalAuthor` variable in the companion file using custom script in the first workflow step, and specify the custom variable in the token instead of using `dDocAuthor`.

The event script in the first step might look like the following:

```
<$wfSet("originalContributor", dDocAuthor)$>
<$wfSet("type", user)$>
```

And the token script for the notification step would look like:

```
<$wfAddUser(wfGet("originalContributor"), wfGet("type"))$>
```

Example 6-3 Reviewers Selected Based on Jump Criteria

One typical use for tokens is to select reviewers as needed, or based on the conditions of a jump. Suppose you have a workflow set up for standard routing of all marketing materials through the Marketing department. However, you want any changes to your company catalogs to also be reviewed by the Distribution department.

To do this, create a jump that adds a token to the list of reviewers whenever the Type is `catalog`. For example:

```
<$wfAddUser("Dist_Dept", "alias")$>
```

Example 6-4 Conditional Token

Rather than creating a jump script for the previous example, you could define a conditional token that adds the `Dist_Dept` alias whenever the Type is `catalog`. For example:

```
<$if dDocType like "catalog"$>
  <$wfAddUser("Dist_Dept", "alias")$>
<$endif$>
```

Example 6-5 Token Specifying Management Chain

Another common use for tokens is specifying the current user's manager as a reviewer. (The manager attribute must be specified as a user information field in Content Server, or as a user attribute in an external directory such as LDAP or ADSI.) For example:

```
<$wfAddUser(getUserValue("uManager"), "user")$>
```

6.5.3 Workflow Jumps

Jumps are used to customize workflows. They are usually a conditional statement, written in Idoc Script.

Typical uses of jumps include:

- Specify multiple metadata fields as the criteria to enter a workflow.
- Take action on content automatically after a certain amount of time has passed.
- Define different paths for files to move through the same workflow depending on metadata and user criteria.
- Release a workflow document before approval by using the side effect: *Release document from edit state*.

The following is an example of a jump that exits the workflow if the author is *sysadmin*:

```
<$if dDocAuthor like "sysadmin"$>
  <$wfSet("wfJumpName", "Entry step")$>
  <$wfSet("wfJumpTargetStep", wfExit(0, 0))$>
  <$wfSet("wfJumpEntryNotifyOff", "0")$>
<$endif$>
```

In most cases, a jump includes a conditional statement. However, a jump can consist of non-conditional code, such as the following:

```
<$wfSet("custom_wf_variable", new_value)$>
  <$wfSet("wfJumpTargetStep", step_1)$>
```

This type of jump can be used to execute code or move a revision to another step automatically.

This section discusses the following topics about jumps:

- Jumps and Events
- Creating a Jump
- Changing a Jump
- Jump Examples
- Jump Errors

6.5.3.1 Jumps and Events

As mentioned in Events, each step in a workflow has an entry, update, and exit event.

A script can be created with one or more jumps for any or all of the events in a step. Any Idoc Script defined for an event is evaluated at a specific time that depends on the type of event:

- An **entry event script** is evaluated upon entering the step. Every time a step is entered, a default script is evaluated in addition to any user-defined custom script. The default script keeps track of the number of times the step has been entered (`entryCount`) and the last time the step was entered (`lastEntryTs`).

  If the entry event script does not result in a jump or exit, any users, aliases, and tokens are evaluated, and email notifications are sent.

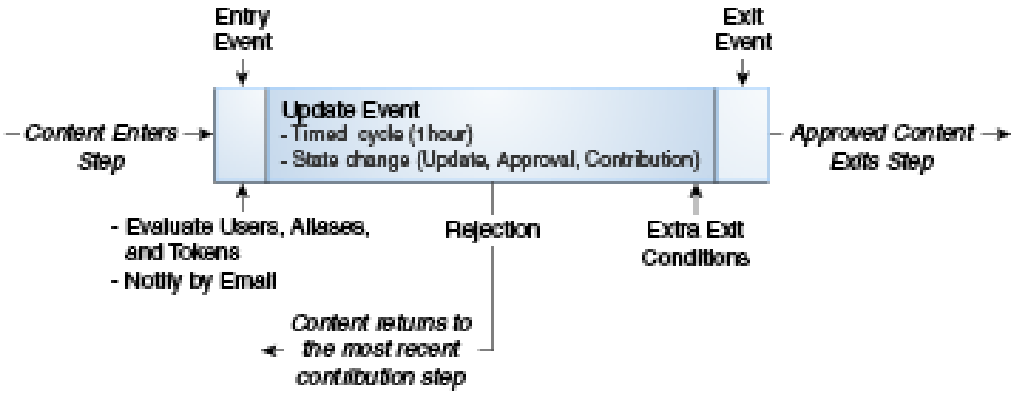
- An **update event script** is evaluated and triggered by a state change of the content, such as the workflow update cycle, the update of the revision's metadata or approval or check in of the revision.

  Extra exit conditions are evaluated each time the update event script is evaluated.

- An **exit event script** is evaluated when a revision has completed the step's approval requirements and the step's extra exit conditions are met.

By default, the workflow update cycle occurs hourly. The cycle time can be increased in increments of one hour (using the `WorkflowIntervalHours` configuration setting), but cannot be reduced to less than one hour. To have update scripts evaluated more often or in response to other events, initiate a metadata update cycle without changing any metadata.

Figure 6-3 Jumps and Events



Within a single workflow, when a reviewer rejects a revision the content item is routed back to the most recent contribution step. However, when a jump is made to a sub-workflow or other workflow and content is rejected there, different behavior occurs. The process returns to the parent workflow, not to the previous contribution step.

> **Important:**
>
> Update and exit event scripts of the current step are not run when a revision is rejected. Any code that is to be evaluated upon rejection must be located in the entry event script for the step that the rejected file is sent to.

Side effects are the actions that take place when a revision in a workflow step meets the jump condition. Side effects can include:

- Jump to another step in the same workflow
- Jump to a step in a sub-workflow or other Criteria workflow (for Criteria workflows only)
- Notify users
- Exit the workflow
- Set state information in the companion file
- Release a workflow document before approval

A jump can include a *target step*, which tells the workflow where to go to if the content meets the jump condition. The following is an example of a target step that sends the content to the next step in the workflow

```
<$wfSet("wfJumpTargetStep", wfCurrentStep(1))$>
```

A jump can also include a *return step*, which tells the workflow where to go if the content is returning from another workflow. The following is an example of a return step that sends the content to the next step in the workflow:

```
<$wfSet("wfJumpReturnStep", wfCurrentStep(1))$>
```

A *step name* variable, `step_name@workflow_name`, is assigned to each step in a workflow. There are two ways to reference a step in a jump:

- **Explicit** reference is made to a specific step name, such as `Editor@Marketing Brochures`.
- **Symbolic** reference is made relative to the current step and workflow, such as `wfCurrentStep(-1)` (previous step) or `wfStart` (first step in the workflow).

> **Tip:**
>
> Use symbolic references rather than explicit step names whenever possible especially when creating a script template.

The *entry count* variable, `entryCount`, keeps track of how many times a step has been entered and is part of the default entry script that is updated each time a step is entered. The following is an example of how an entry count variable is used in a conditional statement:

```
<$if entryCount =1$>
```

The *last entry* variable, `lastEntryTs`, keeps track of when the step was last entered and is part of the default entry script that is updated each time a step is entered. The following is an example of how the last entry variable is used to specify that action should occur if the step has not been acted on within seven days:

```
<$if parseDate(wfCurrentGet("lastEntryTs")) < dateCurrent(-7)$>
```

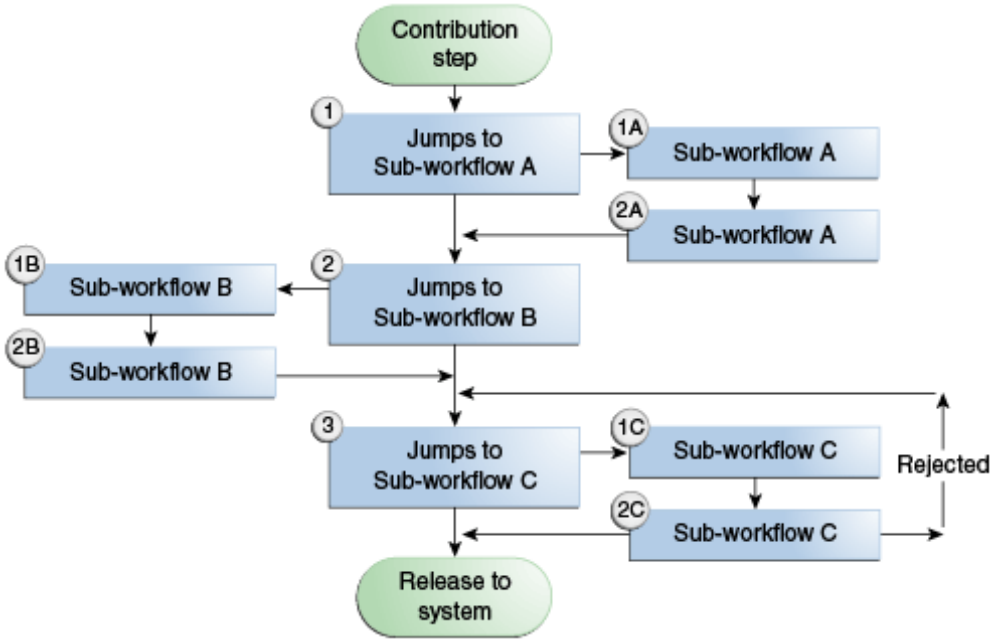
6.5.3.2 Creating a Jump

Before creating jumps, draw a flowchart and work out all the possible jump scenarios. A recommended method of structuring jumps is to create a main workflow with steps that jump to sub-workflows.

Figure 6-4 shows a sample workflow with three sub-workflows: A, B, and C. Sub-workflow C is different because if the result is rejected, then it loops back to the start of the sub-workflow and does not go to the next step (release to system) unless the sub-workflow result is accepted.

After determining what jumps must occur within a workflow, set up the jumps then test them. You can create jumps directly in an existing workflow, or you can create script templates for jumps to be reused in different workflows.

Figure 6-4 Sample Jump Flowchart



6.5.3.2.1 Creating a Jump

To create a jump:

1. Create the workflow that contains jumps. For more information, see Setting Up a Criteria Workflow or Setting Up a Basic Workflow.
2. On the Workflow Admin page, select the workflow. Click the **Criteria** tab or the **Workflows** tab (depending on the type of workflow).
3. In the Steps pane, click **Add** or select the step to include the jump and click **Edit**.
4. On the Add New/Edit Step page, click the **Events** tab.
5. Click **Edit** next to the event (entry, update, or exit) containing the jump.

- If a script template does not exist, use the Script Properties page to add properties.
- If a script template exists, on the Edit Script for StepName page, select an editing option. To create the script from a blank page, select **Create New**. To create the script from a script template, select **Use Script Template** then select a template from the list.

6. Click **OK**.

6.5.3.2.2 Testing the Side Effects of a Jump

To test the side effects of a jump:

1. On the **Jumps** tab, click **Add**, or select an existing jump and click **Edit**.
2. For a new jump, on the Edit Script for StepName page, enter a jump name. You cannot change the Jump Name after you create the jump. Try to use a meaningful, descriptive name.
3. If the jump must specify a return point, select the **Has Return Point** check box and select a return point from the list. The possible options are: Current Step, Next Step, Previous Step.
4. If the reviewers for this step should not be notified when the jump is entered, select the **Do not notify users on entry** check box.
5. If the content item is released before approval, select the Release document from edit state check box.
6. Enter any custom side effects in the **Custom Effects** field. For examples, see Jump Examples.
7. If the reviewers are notified when the jump is entered, click the **Message** tab and enter the notification message.
8. Click **OK**.

   The Edit Script page is re-displayed.

6.5.3.2.3 Setting Up Conditional Statements

To set up conditional statements:

1. Select a metadata field from the **Field** list. This value is the workflow conditions or metadata field to be evaluated.
2. Select an operator from the **Operator** list. **Operator** is a dependent list that shows only the operators associated with the Field.
3. Select a value from the **Value** list. **Value** is the value associated with the specified metadata field.
4. Click **Add** to add the conditional statement to the script.

6.5.3.2.4 Completing the Jump

To complete the jump:

1. If the jump must specify a target step:
   - To specify a specific step, click **Select**, then select the workflow and step name on the Select Target Step page. The target step name is displayed in the target step area.

- To select a symbolic step, such as the current step or exit the workflow, select the step from the **Target Step** list.

2. To modify the script that was just created, click the **Custom** tab, select the **Custom Script Expression** check box, and edit the code.

> **Caution:**
>
> If **Custom Script Expression** is deselected, the expression reverts to its original definition. All modifications are lost.

6.5.3.2.5 Testing the Script

To test the script:

1. Click the **Test** tab.
2. Click **Select**.
3. To narrow the content list, on the Content Item View page, select the **Use Filter** check box, click **Define Filter,** select the filter criteria, and click **OK**.
4. Select a content item to test and click **OK**. Check in and process a test document so that it is in the workflow and at the step you are adding the jump to, then select that content item for testing. If the selected content item is not currently in a workflow, you can still use it to test the script, but it is treated as if it were newly in the workflow.
5. Click **Load Item's Workflow State**.

   If the selected content item is in a workflow, the companion file is loaded in the Input Data field.
6. Click **Test Script**.
7. The test results are displayed in the **Results** field.
   - The value of each parameter in the script is displayed.
   - If any Idoc Script errors occur, they are displayed with the script containing the errors.
8. To save the script, click **OK**.
9. Continue adding jumps as needed to different steps.

6.5.3.3 Changing a Jump

To change an existing jump:

1. Select the workflow on the Workflow Admin page or the **Workflow Admin: Workflows** tab.
2. In the Steps pane, select the step that includes the jump to be changed.
3. Click **Edit** in the Steps pane.
4. On the Add New/Edit Step page, click the **Events** tab.
5. To delete a jump, click **Clear** in the corresponding event pane. To change a jump, click **Edit** in the corresponding event pane.

6. On the Edit Script for StepName page, select an editing option:
   - To edit the existing script, select **Edit Current**.
   - To create a script, select **Create New**.
   - To use a script template, select **Use Script Template** then select a template from the list.
7. On the Script Properties page, click **Add**, **Edit**, or **Delete** in the Jumps pane to change the jump side effects.
8. Use the Field, Operator, Value fields and **Add** and **Update** buttons in the Script Clauses pane to change the conditional statements for the jumps.
9. Use the **Target Step** list to change the target step for the jump.
10. To change the automatically generated script, click the **Custom** tab, select the **Custom Script Expression** check box, and edit the code.

> **Caution:**
>
> If you clear the Custom Script Expression check box, the expression reverts to its original definition and modifications are lost.

11. Test the script before saving it.
12. Click **OK** to save the changes.

6.5.3.4 Jump Examples

The following examples describe how to set up different types of jumps.

Example 6-6 Metadata Criteria Jump

Suppose you have a Criteria workflow called *Marketing Brochures* that is defined with the *Marketing* security group and the *MktBrochure* content type. However, any brochures submitted by a graphic artist do not have to go through the first step, which is graphics department approval. You would use the Edit Script page to create the following entry event script for the first step.

```
<$if dDocAuthor like "bjones" or dDocAuthor like "sjames"$>
  <$wfSet("wfJumpName", "BypassGraphics")$>
  <$wfSet("wfJumpTargetStep", wfCurrentStep(1))$>
  <$wfSet("wfJumpEntryNotifyOff", "0")$>
<$endif$>
```

To change the automatically generated conditional statement from `and` to `or`, you must edit the script on the **Custom** tab of the Edit Script page.

Example 6-7 Time-Dependent Jump

Suppose you want to limit the review period to one week. If the revision has not been approved or rejected, you want to notify the reviewers and process the revision through a sub-workflow called *ApprovalPeriodExpired*. You would use the Edit Script page to create the following update event script:

```
<$if parseDate(wfCurrentGet("lastEntryTs")) < dateCurrent(-7)$>
  <$wfSet("wfJumpName", "LateApproval")$>
  <$wfSet("wfJumpTargetStep",
```

```
    "NotifyAuthor@ApprovalPeriodExpired")$>
  <$wfSet("wfJumpMessage", "The review period for content item
    <$eval(<$dDocTitle$>)$> has expired.")$>
  <$wfSet("wfJumpReturnStep", wfCurrentStep(0))$>
  <$wfSet("wfJumpEntryNotifyOff", "0")$>
<$endif$>
```

6.5.3.5 Jump Errors

Two responses are possible to a jump error:

- An event script that causes an error in execution is treated as if it had never been evaluated. However, the default entry script that keeps track of the entry count and last entry is still evaluated.
- A jump to an invalid step or a step in an inactive workflow results in an error, and the revision is treated as if it has completed the last step of the workflow.

6.6 Workflow and Script Templates

Workflow templates are a quick way to reuse workflows you have created. Each workflow template is an outline for a Basic, Criteria, or sub-workflow that is stored in the Workflow Admin tool. A workflow template is not tied to a security group, and it cannot include step event scripts. Use Script templates to store step event scripts.

The procedure used to create a template is similar to creating a workflow. This section provides an overview of the process. For more information, see Setting Up a Criteria Workflow or Setting Up a Basic Workflow.

This section contains the following topics:

- Creating or Modifying a Workflow Template
- Creating a Script Template

> **Important:**
>
> When you use a workflow template, change the reviewers if they are different from those defined in the selected template.

6.6.1 Creating or Modifying a Workflow Template

To create or modify a workflow template:

1. Display the **Workflow Admin: Templates** tab.
2. To create a new template, click **Add**. To modify an existing template, select the template and click **Edit**.
3. On the Add/Edit Template page, enter a template name in the **Template Name** field. You cannot change the Template Name after you create the template.
4. Enter a detailed description in the **Description** field.
5. Specify whether to permit the original author to edit the existing revision or create a new revision if the content item is rejected by checking the appropriate box.

6. To Add a step, click **Add**.
7. Enter an appropriate **Name** and **Description** for the step.
8. Specify the authority level of the users for the step: Users can review the current revision, Users can review and edit (replace) the current revision or Users can review the current revision or create new revision.
9. Click **OK**.
10. Select the type of users for the step. You can define multiple types of user for a step.
11. Click **OK**.
12. Click the **Exit Conditions** tab.
13. Specify how many reviewers must approve the revision before it passes to the next step.
14. Specify additional exit conditions if needed.
15. If the workflow requires conditional steps or special processing, click the **Events** tab and add the appropriate scripts.
16. Click **OK**.

6.6.2 Creating a Script Template

Script templates are a quick way to reuse step event scripts. A script template is used as a starting point for creating event scripts. Each script template is a piece of Idoc Script stored in the Workflow Admin tool.

> **Note:**
>
> Script templates should use symbolic step names rather than explicit references.

To create a script template:

1. In The Workflow Admin page, select **Script Templates** from the Options menu.
2. Click **Add**.
3. On the Add/Edit Script page, enter a script name in the **Script Name** field. The name cannot be changed after it is created.
4. Enter a detailed description in the **Description** field.

6.6.2.1 Setting Up Jump Side Effects

1. On the **Jumps** tab, click **Add**.
2. Enter a jump name. The name cannot be changed after creating the jump.
3. If the jump must specify a return point, select the **Has Return Point** check box and select a return point from the list.
4. If users should not be notified when the jump is entered, select the **Do not notify users on entry** check box.
5. If the content item is released before approval, select the Release document from edit state check box.

6. Enter any custom side effects in the **Custom Effects** field.
7. If users are notified when the jump is entered, click the **Message** tab and enter the notification message.
8. Click **OK**.

6.6.2.2 Setting Up Script Template Conditional Statements

1. Select a metadata field from the **Field** list.
2. Select an operator from the **Operator** list.
3. Select a value from the **Value** list.
4. Click **Add** to add the conditional statement to the script.

6.6.2.3 Testing the Script

1. Click the **Test** tab.
2. Click **Select**.
3. To narrow the content list, on the Content Item View page, select the **Use Filter** check box, click **Define Filter,** select the filter criteria, and click **OK**.
4. Select a content item to test and click **OK**. If the selected content item is not currently in a workflow, it can be used to test the script but it is treated as if it were newly in the workflow.
5. Click **Select Workflow**.
6. On the Select Workflow Step page, select a workflow in the Workflows pane, select a step in the Steps pane, and click **OK**. Select a workflow step that is similar to the ones for which the script template is used.
7. Click **Load Item's Workflow State**.

   If the selected content item is in a workflow, the companion file is loaded in the Input Data field.
8. Click **Test Script**.
9. The test results are displayed in the Results field.
   - The value of each parameter in the script is displayed.
   - If any Idoc Script errors occur, they are displayed with the script containing the errors.
10. To save the script template, click **OK**.

6.6.2.4 Changing a Script Template

To change an existing script template:

1. On the Workflow Admin page, select **Script Templates** from the Options menu.
2. On the Workflow Scripts page, select the script template to change.
3. Click **Edit**.
4. On the Add/Edit Script page, click **Add**, **Edit**, or **Delete** in the Jumps pane to change the jumps.

5. Use the Field, Operator, Value fields and **Add** and **Update** buttons in the Script Clauses pane to change the conditional statements for the jumps.
6. Use the **Target Step** list to change the target step for the jump.
7. To modify the automatically generated script, click the **Custom** tab, select the **Custom Script Expression** check box, and edit the text.

> **Caution:**
>
> If you clear the Custom Script Expression check box, the expression reverts to its original definition and modifications are lost.

8. Test the script before saving it. For more information, see Creating a Jump.
9. Click **OK** to save the changes.

6.6.2.5 Deleting a Script Template

To delete an existing script template:

1. On the Workflow Admin page, select **Script Templates** from the **Options** menu.
2. On the Workflow Scripts page, select the script template to delete.
3. Click **Delete**.
4. On the confirmation page, click **Yes**.

6.7 Workflow Scenarios

The following workflow scenario describe the planning process and the types of actions required to accomplish specific workflow tasks. It includes the following workflow examples:

- Scenario 1: Criteria Workflow. For information about the steps used to set up a criteria workflow, see Setting Up a Criteria Workflow.
- Scenario 2: Tokens. For information about creating tokens, see Creating, Editing, or Deleting a Token.
- Scenario 3: Jump Based on Metadata. For information about setting up a jump, see Creating a Jump.
- Scenario 4: Time-Dependent Jump. For information about using variables to set jumps, see Creating a Jump.

6.7.1 Scenario 1: Criteria Workflow

Your Marketing department wants to have all marketing brochures approved by at least one of three graphic artists, the editor, and all of the marketing supervisors. The graphic artists and editor can edit the content, but the supervisors should not have editing privileges.

To set up the workflow for this example, you would:

- Define a security group called *Marketing*, and ensure that the graphic artists and the editor have Write permission, and the marketing supervisors have Read permission to the security group.

- Define a content type called *MktBrochure.*
- Define a workflow called *Marketing Brochures*, with the security group set to *Marketing* and criteria set to Type =*MktBrochure*.
- Define the first step, called *Graphic Artist*, as a Reviewer/Contributor step with approval required from at least 1 reviewer. Because the graphics department is very stable, you can assign the user logins of the three graphic artists to the step.
- Define the second step, called *Editor*, as a Reviewer/Contributor step. Assign the editor's user login to the step.
- Define the third step, called *Marketing Team*, as a Reviewer step with approval required from all reviewers. The management structure changes frequently, so set up an alias called *MktTeam* and assign it to this step.
- All marketing brochures must be checked in to the *Marketing* security group with a Type of *MktBrochure*, so it is a good idea to instruct all possible contributors of marketing brochures about how to check them in.
- For the approval process to work correctly, the *MktTeam* alias must be kept up-to-date.

6.7.2 Scenario 2: Tokens

After you created the *Marketing Brochures* workflow in Scenario 1, the Marketing department requested that all marketing brochures be returned to the original author for final review before they are released. The original author should not have editing privileges.

To set up the workflow for this example, you would:

- Create a token called *Author* and define the user as `dDocAuthor`.
- Define a fourth step in the workflow, called *Original Author*, as a Reviewer step. Assign the *Author* token to the step.

6.7.3 Scenario 3: Jump Based on Metadata

The *Marketing Brochures* workflow you created in Scenarios 1 and 3 is working smoothly, but now the Marketing department would like to automatically notify the various sales reps when a new brochure is released for one of their product lines.

To set up the workflow for this example, you would:

- Define a required custom metadata field called *Product*, and create a list of the products.
- Set up an alias for each product, and assign the appropriate sales reps to each alias. You can assign each user to multiple aliases.
- Define a fifth step in the workflow, called *Notify Sales*, as a Reviewer step with approval required from zero (0) reviewers.
- Define a sub-workflow for each product that contains one Reviewer step with approval required from zero (0) reviewers. Assign the corresponding product alias to the step.
- Define an entry script in the *Notify Sales* step that jumps to the sub-workflow that matches the product.

- For the notification process to work correctly, the product list and aliases must be kept up-to-date.

6.7.4 Scenario 4: Time-Dependent Jump

The Marketing department is having trouble getting marketing brochures approved quickly. They would like to change the *Marketing Brochures* workflow to automatically move content to the next step if it hasn't been approved or rejected by the graphics department, supervisors, or original author within 7 days. The editor is allowed a little more time. They get 10 days before the content goes to the next step.

To set up the workflow for this example, you would:

- Define a script template called *AutoApprove*, with a target step that goes to the next step in the workflow if the last entry was 7 days ago.
- Add an update jump to the *Graphic Artist*, *Marketing Team*, and *Original Author* steps. Use the *AutoApprove* script template to create the jump.
- Add an update jump to the *Editor* step, using the *AutoApprove* script template. Edit the script so that the jump occurs at 10 days rather than 7 days.

6.8 Workflow Tips and Tricks

This section describes workflow tips and tricks:

In addition to this functionality, additional customizations are available through Consulting Services. For more information, see Other Customizations.

6.8.1 Requiring Step Authentication

It is sometimes necessary to re-authenticate a user for particular step of a workflow. For each workflow step that requires authentication before approval:

1. Add the following line to the `IntradocDir/config/config.cfg` file:

   <*workflow step name*>`:isRepromptLogin=true`

   If multiple workflow steps require validation, add those steps on separate lines.
2. Restart Content Server.
3. Set up and enable the workflow, making sure to use the step name designated in the configuration entry for the step where validation is required.

When the workflow is initiated, the users at the workflow step designated with the `isRepromptLogin` configuration variable are prompted to login in before they can approve the content at the workflow step.

In the following example, validation is required at the steps named *VIPApproval* and *CEOsignoff*. The following entries are added to the `config.cfg` file:

```
VIPApproval:isRepromptLogin=true
CEOsignoff:isRepromptLogin=true
```

Content Server is restarted and a workflow is set up and enabled with steps named *VIPApproval* and *CEOsignoff*. Multiple users are assigned to the *VIPApproval* step, and only one user (the CEO of the company) is assigned to the *CEOsignoff* step.

Before the users at those steps can approve the workflow item, they must login again.

This functionality is available in Content Server 7.5 and later versions.

6.8.2 Setting Up Parallel Workflows

It is sometimes desirable to have two distinct groups of users able to review content items in workflow at the same time and to have a specified number of users from each group approve the content before it proceeds in the workflow.

When using Content Server, either all users or a specified number of users must approve the content before it continues. Usually the workflow does not differentiate between sources of approval. Consequently, all members of one group approve content while none of another group approve it, and the content would still advance through the workflow. The following code provides an example of how to add approval process discrimination.

This code allows step users to be set into groups. At each approval, the script checks for the group to which a user belongs. A user can belong to multiple groups; if the approving user is in a group, the counter for that group is incremented by one.

Extra exit conditions hold the content in the step until the extra conditions are met.

Add the following code in the **entry** portion of the step:

```
<$wfSet("set1", "0")$>
<$wfSet("set2", "0")$>
<$group1 ="user1, user2, user3,"$>
<$wfSet("group1", group1)$>
<$group2 ="user8, user9, user10,"$>
<$wfSet("group2", group2)$>
```

Add the following code in the **update** portion of the step:

```
<$if wfAction like "APPROVE"$>
<$if strIndexOf(wfGet("group1"), dUser) >=0$>
<$set1 =toInteger(wfGet("set1"))+1$>
<$wfSet("set1", set1)$>
<$endif$>
<$if strIndexOf(wfGet("group2"), dUser)>=0$>
<$set2 =toInteger(wfGet("set2"))+1$>
<$wfSet("set2", set2)$>
<$endif$>
<$endif$>
```

Add the following code in the **extra exit conditions** portion of the step (where *n* is the number of required approvers from group 1 and *r* is the number of required approvers from group 2):

```
toInteger(wfGet("set1")) >= n
toInteger(wfGet("set2")) >= r
```

By checking the approving user during each approve action, this workflow code increments the counter of the group to which the user belongs. The extra exit conditions hold the content item in the step until the minimum number of users in each group have approved it. If more than the minimum number of required approves for each group are executed, the approve actions are still logged but the content item does not proceed.

Reject actions are still absolute. A rejection from any named user still executes normal workflow reject behavior.

6.8.3 Adding Ad Hoc Step Users

You can add users to workflow steps without using metadata fields normally accessed by tokens. For example, a content item is traveling (and being edited) in workflow; each edit lists the person editing the content as the dDocAuthor. To send the item to the original author after the workflow cycle, a special token must be created:

```
<$wfAddUser(wfGet("originalContributor"), wfGet("type"))$>
```

Add the following code to the **entry event** of the first step in the workflow to restore the original author:

```
<$originalContributor=dDocAuthor$>
<$wfSet("originalContributor",originalContributor)$>
<$type="user"$>
<$wfSet("type",type)$>
```

The event script uses `wfSet()` to put custom variables and values into the companion file at a point before the token call. The token then uses `wfGet()` to pull out those values and set the step user.

You can use this technique to obtain and store any standard or custom Idoc variable that holds valid user names or aliases. The Idoc variable can contain a comma-delimited list of user names or aliases. If user names are being stored, the `<$type$>` variable must be set to *user* (for example, `<$type="user"$>`. If alias names are being stored, the `<$type$>` variable must be set to *alias* (for example, `<$type="alias"$>`.

When placed in the entry event of a workflow step with the token set as the step user, the entry event code processes the information. It stores the user name (or alias) which is then called by the token and is set as a step user (or users, if a list was specified). Adding multiple or conditional code blocks and tokens (as shown previously) to your step entry events and step user definitions allows true ad hoc workflow routing.

6.8.4 Customizing Criteria Workflow Emails

Emails are triggered by criteria workflow at three points in the process:

- On entry to a step.
- On receipt of a reject reasons form.
- On execution of the `wfNotify` Idoc Script function.

It is possible to customize the email message, the email subject, and the template used for emails sent during criteria workflows. This section describes the processes for customizing the email aspects of criteria workflows.

This section includes the following topics

- Customizing Email Templates
- Customizing the Subject or Message Line

6.8.4.1 Customizing Email Templates

The two most commonly used templates used to generate email messages sent to recipients involved in a workflow are *reviewer_mail.htm* and *reject_mail.htm*. These are stored in *IdcHomeDir*`/resources/core/templates`.

You can modify these templates like any other template. Email template modification provides the greatest flexibility and opportunity for customizing workflow emails. Although this kind of modification is relatively straightforward, it still requires careful component development. Modifying the subject and the message in the email is often the most important part of the message, and thus is often the most modified.

Custom workflow email templates based on the standard templates can also be created. To call custom templates, add them as the optional third parameter to the `wfNotify` function, as in these examples:

```
<$wfNotify(userName, "user", templateName)$>
<$wfNotify(aliasName, "alias", templateName)$>
```

If an alternate template is not specified, the system default template is used.

For more information, see the discussion of `wfNotify` in *Configuration Reference for Oracle WebCenter Content*.

6.8.4.2 Customizing the Subject or Message Line

You can customize criteria workflow email subject and message lines for your application.The email subject line appears in the email; the message line appears in the email body with other information about the workflow email (workflow name, step, and content item).

The message line defaults to one of two messages, depending on whether the step is notification-only (that is, if it has zero required reviewers).

You can customize subject lines and message lines in two ways:

- You can modify the core string resource file according to standard component architecture.
- For simple customizations, you can declare the `wfMailSubject` (for email subjects) or `wfMessage` (for message lines) Idoc Script variable in a criteria workflow step event script or stored in the companion file.

6.8.4.2.1 Modifying Strings

The string definitions are as follows (variable `1` is the content item title and variable `2` is the name of the workflow step):

```
<@wwWfIsNotifyOnly=Workflow notification for content item '{1}' is in step
'{2}'.@>

<@wwWfReadyForStep=Content item '{1}' is ready for workflow step '{2}'.@>

<@wwWfRejected=Content item '{1}' has been rejected.@>
```

You usually call these string definitions with the Idoc Script <$lc()$> localization function and you can alias them in a component resource file. For an example of email subject line string includes, see the <@dynamichtml wf_approve_mail_subject@> include definition in the std_page.htm file.

6.8.4.2.2 Changing Idoc Variables

For simple email or subject line changes, you can use Idoc Script rather than a component. You can place the wfMailSubject configuration variable or the wfMessage configuration variable in step event script. The value of these variables can also accept Idoc Script, as in this example:

```
<$wfMailSubject="My custom subject text for content with <$dDocTitle$> title"$>
```

No eval() function is required for the Idoc Script variables to evaluate.

If wfMailSubject or wfMessage is placed in the entry event of a workflow step, the email messages triggered by content entering the step receives the customized subject or message line. These variables can also be declared before a wfNotify() function and the email then generated by that function receives the customization.

6.8.5 Workflow Escalation

This example requires familiarity with tokens and coding.

Workflow escalation (that is, dynamically routing workflow content to different people than listed users) is a common workflow requirement. While this is easily accomplished with jumps and parsing of some criteria (for example, date, action, metadata) there is often some initial confusion or hesitation about where or to whom the content should go.

The issue is further complicated when the solution is to add a larger number of step users and to require only a subset of those users to approve the content before it can move on. This workflow still generates and sends out emails and appears in the workflow queue of non-approving users, users out of the office, and others who are there "just in case" some primary reviewer is not available.

6.8.5.1 Setting Up a Workflow Escalation

This solution incorporates two custom user metadata fields, a token, and workflow step entry and update event code.

1. Create a user metadata field with the following elements:
   - name: OutOfOffice
   - type: text
   - option list: yes
   - option list type: select list validated
   - option list values: <blank>, false, and true

2. Create another user metadata field with the following elements:
   - name: `OutOfOfficeBackup`
   - type: Long Text

   The `OutOfOffice` field is a flag that the user sets as TRUE when they are out of the office. To set this flag, select **TRUE** from the list and click **Update** to update the user profile.

   The `OutOfOfficeBackup` field contains the user name(s) of those users who can fill in as proxies for the out-of-office user. This field should optimally contain a single user name, formatted as shown in the User Admin applet.

   When the following workflow step event code finds that a listed user is "out of the office" it switches that user's name for the listed proxy (as designated by the value in the `OutOfOfficeBackup` field). The workflow step then restarts with only the users who had not yet approved the content and any designated proxies.

   A token pulls the list of users out of the companion file and sets them as step users. Special workflow messages are sent to designated proxies while the content was sitting in the update step event.

3. Create a workflow Token
   - name: `DynamicStepUsers`
   - Token Code:

   ```
   <$if wfGet("dsu")$>
     <$wfAddUser(wfGet("dsu"), "user")$>
   <$else$>
     <$wfAddUser("sysadmin", "user")$>
   <$endif$>
     <$if wfGet("dsa")$>
        <$wfAddUser(wfGet("dsa"), "alias")$>
   <$endif$>
   ```

   The token pulls a value for the custom variable `dsu` and `dsa` out of the companion file. If no value is found for `dsu` then the *sysadmin* user is added as a precaution. The initial values for `dsu` and `dsa` are listed in the entry event of the step. If you want to assign users to the step(s), add the first contributor to the first step and the next step must include the first user plus the next user, user two.

4. Paste the following code into the **entry** event of your workflow step. Comments are included through the entry code; remove the comments before inserting into your step:

   ```
   <$restartFlag=wfGet("restartStep")$>
   ```

   See if the cause is a restart for new backup users. If so, suppress notifications to old users and notify only new ones

   ```
   <$if restartFlag$>
   <$if toInteger(wfGet("restartStep"))>=1$>
     <$wfSet("wfJumpEntryNotifyOff", "1")$>
     <$oooUsers=wfGet("outOfOfficeUsers")$>
     <$if strIndexOf(oooUsers,",")>=1$>
   ```

   Check for multiple out of office users

   ```
     <$wfMessage=eval("The Following Users are out of the office:
   <$oooUsers$>
   ```

```
  \nYou are the designated backup for one of them.\n
  The content item <$dDocName$> is in the workflow step <$dwfStepName$>
awaiting your   review")$>
<$else$>
  <$wfMessage=eval("The Following User is out of the office: <$oooUsers$>
  \nYou are the designated backup for this user.\n
  The content item <$dDocName$> is in the workflow step <$dwfStepName$>
awaiting your   review")$>
<$endif$>
<$rsMakeFromString("ooou",oooUsers)$>
<$loop ooou$>
  <$userBackupName=row&"_Bkup"$>
  <$wfNotify(wfGet(userBackupName),"user")$>
<$endloop$>
<$wfSet("restartStep","0")$>
<$endif$>
    <$else$>
<$wfSet("restartStep","0")$>
  <$endif$>
```

Set your step users here. Multiple users must be comma-delimited, user names must be in quotes, metadata field references are unquoted. This example proceeds, using user names rather than aliases. Slight code re-working is required if using aliases.

```
<$dynamicStepUsers= <LIST USER NAMES IN QUOTES HERE>$>

<$if strIndexOf(dynamicStepUsers,",")>=1$>
```

If there are multiple users specified verify if any of the MULTIPLE users are out of the office

```
<$rsMakeFromString("multiDynamicUsers",dynamicStepUsers)$>
<$loop multiDynamicUsers$>
  <$if strEquals(getValueForSpecifiedUser(row,"uOutOfOffice"),"true")$>
```

If user is out of office, get their backup

```
  <$backup=getValueForSpecifiedUser(row,"uOutOfOfficeBackup")$>
```

Replace out-of-office user in users list with their backup

```
  <$dynamicStepUsers=strReplace(dynamicStepUsers,row,backup)$>
  <$endif$>
  <$endloop$>
   <$else$>
```

Verify if the SINGLE user is out of the office

```
  <$if
strEquals(getValueForSpecifiedUser(dynamicStepUsers,"uOutOfOffice"),"true")$
>
```

If user is out of office, get their backup

```
<$dynamicStepUsers=getValueForSpecifiedUser(dynamicStepUsers,"uOutOfOfficeBa
ckup")$>
  <$endif$>
<$endif$>
<$wfSet("dsu",dynamicStepUsers)$>
```

Set the dsu variable into the companion file with listed and backup users

5. Paste the following code into the **update** event of your workflow step, removing comment lines before doing so:

```
<$remainingUsers=wfGet("wfUserQueue")$>
```

Get users who have yet to approve

```
<$rsMakeFromString("ru", remainingUsers)$>
<$loop ru$>
<$if strEquals(getValueForSpecifiedUser(row,"uOutOfOffice"),"true")$>
```

Check the remaining users to see if they are out of the office

```
<$if getBackup$>
```

Create list of users requiring backup substitutes

```
  <$getBackup=row &","&getBackup$>
<$else$>
  <$getBackup=row$>
<$endif$>
<$endif$>
<$endloop$>
<$if getBackup or strLength(getBackup)>0 $>
```

If a user is listed as out of office then rewrite the user list and restart the step

```
<$wfSet("outOfOfficeUsers",getBackup)$>
<$rsMakeFromString("needBkup", getBackup)$>
<$loop needBkup$>
<$bkupUser=getValueForSpecifiedUser(row,"uOutOfOfficeBackup")$>
<$newRemainingUsersList=strReplace(remainingUsers,row,bkupUser)$>
<$wfSet(row&"_Bkup",bkupUser)$>
<$endloop$>
<$wfSet("dsu",newRemainingUsersList)$>
<$getBackup=""$>

<$wfSet("wfJumpTargetStep", wfCurrentStep(0))$>
<$wfSet("restartStep","1")$>
<$endif$>
```

6.8.6 Other Customizations

Many workflow customizations are available through Consulting Services. This section briefly describes two of those customizations. Please consider engaging Oracle Consulting Services for a thorough evaluation of the impact associated with the replication of workflow examples.

The following customizations are discussed in this section:

- Setting Approval by Non-Reviewers
- Automatic Replication of Workflow Items

6.8.6.1 Setting Approval by Non-Reviewers

It is sometimes necessary to have a person approve content in a workflow step even if that individual is not part of the actual workflow. For example, if you want an outside opinion on a document in a particular stage in a workflow or if you want to designate a substitute reviewer because another reviewer is out of the office. The individual can approve content but they do not get normal workflow notifications and do not see the content items in their workflow queues.

Users with designated roles or who are members of designated aliases can approve content on this basis. These designated users see a **Bypass Approve** link in the workflow actions box for each item in a workflow to which they have normal security access. Performing a Bypass Approve approves the content item in the step in which it currently resides. Defined step exit conditions are still evaluated and still apply. The approval is logged in the Workflow History database table and in the WorkflowActionHistory ResultSet of the companion file.

A designated approver is not a regular workflow step approver and thus does not receive automatic workflow notifications. Access to a content item in a workflow where the approver wants to perform a Bypass Approve action must be intentional. The designated approver must access the Active Workflows menu, then select the workflow name and select an action.

The designated approver component aliases core resources. If other components are running or are planned, this must be taken into account. In some cases, you can combine component resources to include all required functionality or you can rename and re-reference them to keep all components working correctly (but separately).

6.8.6.1.1 Scenarios

For the following scenarios, assume that User A has a role or alias that grants designated approver status and that a sample workflow named `MyWF` has two steps.

- Scenario 1: User A is listed as an approver for step 1 in `MyWF` but not in step 2. Therefore, no **Bypass Approve** link appears for Step 1. User A received default workflow action capabilities and notifications. The **Bypass Approve** link for step 2 appears under the Workflow Actions menu if User A accesses the Content in workflow *MyWF*' page when the content item is in step 2.
- Scenario 2: User A is not listed as an approver in `MyWF`. The Bypass Approve link appears in the action menu on the Content in workflow `MyWF`' page for all steps and for all content to which User A has at least Read permission in its Security group.
- Scenario 3: User A is not listed as an approver for Step 1 in `MyWF`. Step 1 requires two approvals from reviewers before it moves to step 2. The **Bypass Approve** link appears for User A. Click **Bypass Approve** to register an approval and fulfill one of two required approvals for the step to continue in the workflow.

6.8.6.2 Automatic Replication of Workflow Items

Content items are often processed (in one form or another) before they are 'released'. A released content item is indexed and can then be included in search results, archives, and in other processes and applications.

It is sometimes useful to release a content item before its completion in the workflow. For example, a content item must be in a released state to be replicated (and perhaps later used in disaster recovery). Items not released (such as items in workflows) are not used by the replicator.

It is possible to designate workflow items as released while still in workflow. Normal workflow actions, such as updating, checking out, and checking in are still available. However, these items are indexed and appear in search results, can be used in replication and archiving, and in any other processes or applications.

> **Important:**
>
> There are several elements to consider before replicating workflow items. This section describes the process but does not go into detail; contact Consulting Services before setting up replication of workflow items.

6.8.6.2.1 Potential Conflicts

There are several points to be aware of before setting up automatic replication:

- Loss of data integrity: A premature release of content, whether intentional or otherwise, can have unforeseen effects on business process management, content accessibility, and information integrity. Potential ramifications must be thoroughly considered before the release of items still in workflow is considered.
- Non-capture of workflow information: Workflows are a combination of process **and** content. While it is possible to release content and make it available for replication and other processes, it is not possible (without customization and assistance from Consulting Services) to capture and replicate workflow *state* information.

  If content in a workflow on a source instance is replicated and released on a target instance without passing through a workflow on that instance, the recovery process involves manual effort to re-set the content's workflow state.

  In most cases, cloning of workflow information is not necessary because recovery to a prior workflow state is required only during true disaster recovery. In all other cases, content items replicate as normal after exiting a workflow and supersede versions or revisions replicated during workflow.
- Imported content items do not enter workflow: Content items replicated while in a workflow on a source instance do not enter a workflow on the target instance without additional customization and assistance from Consulting Services. Replicated content items are checked in to the target instance and released.
- Restoration of replicated workflow items requires manual intervention: You can capture some workflow information as metadata for use in a manual restoration of the workflow. Only a check-in action triggers a content item's entry into workflow. To restore an item back into a workflow requires that you create a revision.

  To recover the content items on the target to a state as close as possible to their previous state on the source, a discrepancy between the number of revisions on the source and the target instances is intentionally and unavoidably introduced.

6.8.6.2.2 Scenarios

For content item 1, *not released while in workflow*, the following is true:

- The content item moves through workflow in a non-released state.
- The content item is not a candidate for replication while in workflow.

- The content item is available only to named workflow step reviewers and administrators.
- When the content item completes the workflow, it is released, indexed, and is now a candidate for replication.

For content item 2, *released while in workflow*, the following is true:

- The content item moves through workflow and is released as specified. After an item is released, it cannot be 'unreleased'. New revisions of a content item created during workflow are not released unless specified.
- Content items released while in workflow display in search results and can be viewed by users with the appropriate security access.
- Users cannot edit, check out, check in, or update a released item that is in workflow unless they are designated users for the step in which the item is located and that step allows the attempted action.
- A content item released while in workflow is a candidate for automatic replication. The Replicator treats the item as if it is not in workflow.
- Content items completing workflow are replicated in the normal fashion and supersede any pre-existing content item versions replicated during workflow.

For information about implications of the release of content items in workflow for replication or other purposes, contact Consulting Services.

6.8.7 Triggering Criteria Workflows from Folders

It is sometimes necessary for documents in a particular folder to go through a criteria workflow. However, when you create a criteria workflow based on a folder, the criteria option of `folder` is not listed in the field list. The field list in criteria workflows only lists fields with a type of `text` or `long text`. Because Folder (xCollectionID) is an integer field, it is not an option.

Although you cannot select the folder field on the Edit Criteria form, you can define it as a criterion in Events. In the Entry Event of the first step, you can set up criteria to check for the appropriate folder number (xCollectionID). If it does not fulfill the criteria, the item can exit from the workflow.

The following general steps detail how to set up such a workflow:

1. Start a new criteria workflow and choose the Security Group that the workflow uses.
2. In the Criteria Definition section, define global criteria to monitor all of the documents that enter the system. For example:

   ```
   Field: ContentID
   Operator: Matches
   Value: *
   ```

   To monitor only items coming in through a specific folder, set an extra metadata field that specifies a folder number.

   If multiple workflows are in place, you can filter all content through this workflow and jump to sub-workflows through multiple criteria settings in the first step of this workflow.
3. Add the first step to the workflow.
4. In the **Events** tab, click **Edit** from the Entry Event.
5. On the **Jumps** tab, click **Add**.

6. Give the jump a meaningful name (for example, Folder Criteria) and click **OK**.
7. For the jump criteria, enter the following:

   ```
   Field: Folder
   Operator: Not Equals
   Value: Folder ID on which the workflow is based
   ```

   When done, click **Add**.
8. For the Target Step, select Exit to Parent Step and change both of the 0 parameters to 10 (for example, `@wfExit(10,10)`. Documents not in the folder are forced out of the workflow.
9. Click **OK** on the Entry Event and click **OK** on the Add New Step dialog.
10. Add the necessary jumps, steps, and events for the rest of the workflow and enable it.

6.8.8 Searching Within a Workflow Step

When executing the GET_SEARCH_RESULTS service within a workflow step, you can experience data corruption because the workflow's data binder is being used by the service.

A solution for this is to temporarily set the security group value into a temporary variable. Then clear the current security group value, make the call for the search results, then reset the security group back again.

6.8.9 Suppressing Workflow Notifications

When a workflow step requires multiple approvers, a user who has approved the document can be re-notified during a timed workflow update cycle. To prevent additional notifications, use the `wfIsNotificationSuppressed` workflow function. Used in a workflow step in the script section of the workflow, it sets an internal flag to determine if workflow notifications are sent out during the current document action (check in, approve, update, and so on). The suppression is applied to both email and updates to the workflow in the queue.

When used in combination with `wfIsFinishedDocConversion`, this function can suppress notification until conversion is finished. It does not prevent documents from advancing out of the auto-contributor step but it does stop updates of the workflow in queue and notification emails.

These notifications are not lost. If the `wfIsNotificationSuppressed` function is not used in a future workflow event to suppress notifications (updates to workflow in queue and workflow mail) then all users participating in the current step are notified.

You can use the following additional functions in the script section:

- `wfIsFinishedDocConversion`, which returns a result indicating if the document is not in GENWWW after the current document action ends.
- `wfIsNotificationSuppressed()`, which returns TRUE if this workflow is currently suppressing all workflow notifications for this particular workflow event.

For information about using these functions, see *Developing with Oracle WebCenter Content*.

You can also suppress all notifications related to a workflow by updating the custom script tag. To suppress all notifications for a user:

1. In a workflow step, navigate to the **Events** tab.
2. Click the **Edit** button of the **Entry** section.
3. Click the **Custom** tab in the Script Properties page.
4. Add the following value to the custom script expression and click **OK**: `<$suppressWorkflowNotification() $>`.

7

Customizing Repository Fields and Metadata

This chapter provides information on managing repository content when there is a need to create custom application fields and custom metadata to tailor input forms and searching. You also can create metadata schemas to manage dependent lists that are localized for specific sites
This chapter includes the following topics:

- Understanding Custom Fields
- Defining an Option List
- Using Schemas to Customize Metadata

7.1 Understanding Custom Fields

Application fields are custom fields that you can use to customize forms and pages. With application fields, you can add features such as dependent lists to forms. You can also use application fields in custom components, HCSP (Hypertext Content Server page) files, and HCSF (Hypertext Content Server Form) files.

By default, application fields do not appear on the standard check-in and search forms, but are used by custom templates. You can use application fields as placeholders or with schema views to enable dependent lists without creating an associated metadata field. For more information, see Using Schemas to Customize Metadata.

You can specify in a content profile which application fields are displayed on the standard check-in and search pages. For more information, see Managing Content Profiles .

Application fields are not indexed and are not searchable. Changes to application fields do not affect the database or the index.

If you use the Electronic Signature component, you can also define custom fields for use with the electronic signature metadata. For more information on Electronic Signature, see Signing Content Electronically.

For each content item, the system maintains a set of information about the content, or *metadata*. Metadata is similar to a card in a library's card catalog, while the actual files are similar to library books. As with the card catalog, metadata consists of information about a file (title, reference number, author, subject, publishing date, book location, and so forth).

In addition to the standard metadata fields provided with the system, you can create new fields to accommodate unique content or system design requirements. It is important to create only the necessary amount of additional metadata necessary to help locate or manage a content item.

When you create a custom field name, the system automatically prefixes the name with an 'x' to ensure that it is unique and does not conflict with any reserved names. Similarly, when you create custom user information (metadata) fields, the system prefixes the name with a 'u' to ensure that it is also unique and does not conflict with any reserved names.

Metadata fields are indexed and searchable. Changes to custom metadata fields can affect the database (where information about metadata fields is stored) or the search index (where the metadata values are stored).

> **Note:**
>
> When using the `DATABASE.METADATA` search engine (the default value is `SearchIndexerEngineName`), there is no search index to manage or query. The data is stored and retrieved using the following tables: `RevClasses`, `Revisions`, `DocMeta`, and `Documents`.

This section covers the following topics:

- Standard Metadata Fields
- Adding or Editing a Custom Field
- Rebuilding the Database or the Search Index

7.1.1 Standard Metadata Fields

The following are standard fields provided with the system. You cannot edit or delete these fields.

Field Caption	Entry Method	Required?	Definition
Content ID	Text Entry or Automatic Generation	Yes	The unique identifier for each content item. • Duplicate names are not allowed. • Maximum field length is 30 characters. • Use only letters, numbers, and underscores (_). Do not use spaces or other special characters. • The Content ID can be automatically generated. For more information, see the **General Options** tab of the System Properties Utility. If using an Oracle or DB2 database, all Content IDs are converted to uppercase letters automatically.
Type	List	Yes	An identifier used to group content. • Types become subdirectories in the *weblayout* directory. • Maximum field length is 30 characters. • Use only letters, numbers, and underscores (_). Do not use spaces or other special characters.
Title	Text Entry	Yes	A descriptive title for the content item. • Maximum field length is 255 characters.
Author	List or Text Entry	Yes	The user who checked in the content item.
Security Group	List	Yes	The security group for which users must have permission to access the content item. • Duplicate names are not allowed. • Maximum field length is 30 characters. • Use only letters, numbers, and underscores (_). Do not use spaces or other special characters.

Field Caption	Entry Method	Required?	Definition
Account	List or Text Entry	No	The account for which users must have permission to access the content item. This field is available only if accounts are enabled.
Primary File	Text Entry or Browse to File	Yes	The complete path to the native file being checked in. Maximum file name length is 80 characters, including the directory path and file extension. Maximum file extension length is eight characters. The Folders option modifies this maximum file name length on installation to 255 characters.
Alternate File	Text Entry or Browse to File	No	The path name to another Web-viewable file format of the native document, or one that can be converted to a Web-viewable format. For example, when checking in a FrameMaker or Quark document that has several files that comprise the document, you would check in a zipped file as the native format (or Primary File) and a Postscript, PDF, or viewable file as its Alternate File. The zipped file is not viewable on the Web, but Inbound Refinery converts the Postscript file to its Web-viewable format, PDF. Maximum file name length is 80 characters, including the directory path and file extension. Maximum file extension length is eight characters. The Folders option modifies this maximum file name length on installation to 255 characters.
Revision	Automatic Generation or Text Entry	Yes	A label (such as 1, 2, 3,... or A, B, C,...) that represents the number of times the content item has gone through its life cycle (the number of revisions). You can customize the Revision label for your revision scheme.
Comments (optional)	User Text Entry	No	A field for additional information about the file. Maximum field length is 255. This field is considered a custom field and can be deleted.
Release Date	Automatic Generation or Text Entry	Yes	The date the file is to be released so it is available for searching and viewing. The Release Date defaults to the date and time the file is checked in.
Expiration Date	Text Entry	No	The date the file is no longer available for searching or viewing. All revisions of the content item expire when the current revision expires. When a content item expires, revisions are retained, but only an administrator can access from the Repository Manager, unless you use *Notification of Expiration*.

7.1.2 Adding or Editing a Custom Field

To add or edit a custom field, either application or metadata field:

1. Use the main menu to choose **Administration** then **Admin Applets**.
2. Click **Configuration Manager**.
3. On the Configuration Manager page, click **Information Fields** to add a metadata field. Click **Application Fields** to add or edit an application field.

   Click **Add** to add a new field or highlight a field. Click **Edit** to change a field.

4. If you are adding a metadata field, enter the name. Duplicate names are not allowed. Maximum field length is 29 characters. Use only letters, numbers, and underscores (_). Do not use spaces or other special characters. Click **OK** when done.
5. On the Add/Edit Metadata Field page or Add/Edit Application Field page, enter or edit the information for the field:
   - Field Caption: The label for the field displayed to users.
   - Field Type: The size indicated is the character input length, not an indication of the actual number of bytes needed to store the field.
     - Integer: -2^{63} to 2^{63} -1. By definition, an integer is a natural number, so decimal values and commas are not permitted.
     - Decimal: -2^{31} to 2^{31} (-2 billion to +2 billion).
     - Memo: 2000 characters.
     - Date: Date format (such as *dd/mm/yyyy* or *dd/mm/yy* for the English-US locale).
     - Long Text: 200 characters.
     - Text: 30 characters.
   - Field Order (metadata fields only): Sequence in which the field is displayed on pages. Starting at 2, the number automatically increments as new fields are added. However, it is recommended to manually increment the numbers by 5, such as 15, 20, 25, and so on to accommodate fields added in the future.
   - Default Value (metadata field only): Any default value for the field.
   - Require Value (metadata field only): Prevents files from being checked in if the field does not have a value.
   - Placeholder: If selected, the field is not stored or indexed. Placeholders are often used for the parent level of a dependent list.
   - Enable on User Interface (metadata field only): If selected, the field is displayed. If deselected the field is hidden.
   - Enable for Search Interface (metadata field only): If selected, the field is indexed and thus used for searching. If deselected, the field is not indexed nor does it appear on the search pages. This will add a column `x{CustomFieldName}` in the `DocMeta` table. By default, an index is not created for that column in the `DocMeta` table because adding indexes are subjective on how that field is used (for example, may not be beneficial to have an index when there are only two distinct values, `yes` or `no`). An index can be created if it is desired to have an index on the metadata field.
   - Enable Option List: Enables the use of user-selectable list on a page. For more information, see Defining an Option List.
   - View Only (application field only): If selected, the field is only used in a schema view. For more information, see Using Schemas to Customize Metadata.
6. Click **OK**.
7. Update the database design and rebuild the search index if necessary.

7.1.3 Rebuilding the Database or the Search Index

The following table lists the events after which a database update or search index rebuild is required depending on the search engine that is used.

> **Note:**
>
> Rebuilding the search index is not required when using the `DATABASE.METADATA` search engine.

Event	Action Required
Add metadata field	Update database
Edit metadata field	Update database
Delete metadata field	Update database
Enable or disable *Enable for Search Index* for metadata field	Rebuild search index
Add metadata field with *Enable for Search Index* selected	Rebuild search index

Rebuilding the Database

If changes were made that must be saved to the database, the **Update Database Design** button on the **Information Fields** tab of the Configuration Manager page becomes active. To update the database:

1. Click **Update Database Design**.
2. To retain a field, deselect the box next to the field name. The field remains hidden but still exists in the database.

   You cannot remove added or edited fields using this page. They must be added then deleted later.
3. Click **OK** when done.

Rebuilding the Index

If changes were made that require rebuilding the search index, the **Rebuild Search Index** button on the **Information Fields** tab of the Configuration Manager page becomes active. To rebuild the search index:

1. Click **Rebuild Search Index**.
2. If a message asks to update the database design before rebuilding the search index, click **Update Database Design** to save changes to the database before proceeding.
3. When the message `Rebuild initiated` is displayed, click **OK**.

> **Caution:**
>
> Depending on the size of the search index and available system resources, the search index rebuild process can take several days. If rebuilding is necessary, rebuild at times of non-peak system usage.

7.2 Defining an Option List

Lists are used with custom fields to provide a selection from which users can choose a value.

Follow these steps to define a list:

1. Create the custom field and click **Enable Option List**, then click **Configure**. For more information, see Adding or Editing a Custom Field.
2. On the Configure Option List page, choose what type of list to use:
   - Multiselect List: Provides a list from which users can select multiple items.
   - Edit and Multiselect List: Provides both a text field and a data entry box. Contributors can enter values that are not in the list and they can select or enter multiple values.
   - Edit and Select List: Provides both a text field and a data entry box. Contributors can enter values that are not in the list.
   - Select List Not Validated: This option permits check in of files whose specified values are not current options. This option is valid for items checked in or updated using the Content Server Interface, the Batch Loader, and the Archiver.
   - Select List Validated: This option ensures that only files whose specified values are current options for this field are checked in. This option is valid for items checked in or updated using the Content Server Interface, the Batch Loader, and the Archiver.

   Click **Advanced** to display the Option List Storage page where information about the list's display and storage are specified. For more information, see Defining Option List Storage.
3. Choose how to access the values in the list:
   - Use Option List: Create a new list or edit an existing values. The name of the new list, taken from the name of the field, is inserted. For more information, see Adding or Editing Option List Content.
   - Use View: Uses values in a stored view instead of a list. Click **Edit Values** to change the values saved in the view. For more information, see Editing View Values.
   - Use Tree: Uses values stored in a tree rather than a view or a list. Click **Edit Definition** to change how the tree is viewed or stored.
4. Determine the dependencies for the list:
   - Dependent field: Check if the metadata field is subordinate to another field. This option is only available when using a view.
   - Depends on: If you select the Dependent Field, this becomes active. Enter a field name or choose the field from the list of fields.
   - Relationship: If a relationship has been defined for the view in use, select it from the list. For more information, see Schema Structure. If you select a list or view, you must specify a relationship.
5. Click **OK** when done.

7.2.1 Defining Option List Storage

One part of creating a list is to determine the storage options. To define storage, click **Advanced** next to the Option List Type on the Configure Option List page. Enter the following information:

- Storage type: Choose to either permanently store list keys or store a localized list.
- Multiselect options: Choose options to customize the appearance of a multiselect list:
  - Pad ends: Pad the length of the separator for multiselect values.
  - Storage Separator: Change the separator used to store values.
  - Display Separator: Change the separator used in the display of values.

Click **OK** when done.

7.2.2 Adding or Editing Option List Content

To open the Option List page, click **Edit** next to the Use Option List field on the Configure Option List page. Enter the following information:

- Option list values: The items to select. Each value must be on a separate line, with a carriage return between values.
- Sort order (ascending or descending): Sorts the list in alpha-numeric order. If ascending, capital letters precede lowercase letters. If descending, the reverse is done. If **Ignore Case** is selected, the list is sorted and the case of the letters is ignored.
- Sort Now: Sorts the list in the manner specified (ascending, and so on).

7.2.3 Editing View Values

A view displays the items available in a list. To edit a view, click **Edit View** next to the **Use View** field on the Configure Option List page. Make the following selections:

- Filter: Select a filter to alter which values are displayed on the page.
- Show Columns: Limits the number of columns to display.
- Add, Edit: Displays a page where you can add or edit new values for those currently in the view.
- Delete: Prompts to confirm the deletion of a value from the view.
- Edit Batch: Displays a page you can use to edit values in a line editor. To add values, enter the data in the appropriate columns separated by a pipe symbol (|). Each row in the table should begin on a new line.

7.2.4 Using Tree Values

A tree displays the items available in a list. If you use this method, make the following selections:

- Select relationship: Choose a relationship between options in the list.
- Remove view: Click to remove the selected view from the level in the tree.

- Selection path: Choose to display the complete path when the option is selected or to save the complete path when the option is selected.
- Separator: Specify the separator used between values.

7.3 Using Schemas to Customize Metadata

To create custom metadata fields that present a list of values, use the **Information Fields** tab of the Configuration Manager utility. You can also make the associated list dependent on the value of another field. This organization is called a *dependent choice list* (DCL).

For example, assume there are Country and State information fields. The country you select determines the choices available in the State list.

You can also use metadata schema mapping to create field lists. With metadata schema mapping, you can easily adjust option list views to accommodate localization requirements.

This section discusses the following topics:

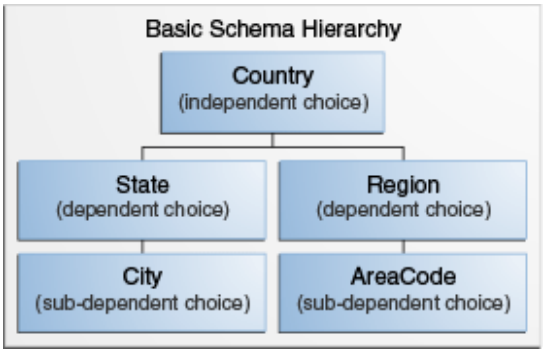
7.3.1 Schema Structure

A *schema* is a collection of related schema objects. The term *schema* also refers to a graphical depiction of the database hierarchy that is created to support the Content Server metadata schema mapping feature. The schema hierarchical structure consists of tables and their respective columns (or fields), views of the data, and the relationships between them.

Let's add City, Region, and Area Code information fields to the Country and State example to illustrate a three-tiered dependency structure.

In Figure 7-1, the sample basic schema hierarchy, one independent field has two dependent fields. Each dependent field also has a dependent field. These dependencies are also referred to as *Parent/Child relationships*.

Figure 7-1 Basic Schema Hierarchy Example



This three-level schema hierarchy produces five distinct metadata fields: Country, State, City, Region, and Area Code. Each field presents a specific list to the user.

The contents of the lists are contingent on whether the information field is dependent or not. Thus, the following lists result from the sample basic Country/State/Area Code schema hierarchy:

- The Country list is independent and the choices remain constant.
- The choices available in the State list are variable and depend on which country the user selects from the Country list.
- The choices available in the City list are variable and depend on which state the user selects from the State list.
- The choices available in the Region list are variable and depend on which country the user selects from the Country list.
- The choices available in the Area Code list are variable and depend on which region the user selects from the Region list

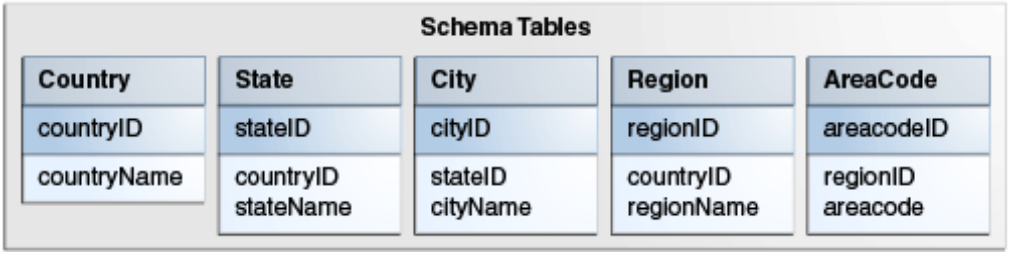
Schemas are comprised of Tablesand Relationships, as discussed in the following sections.

7.3.1.1 Tables

Schema tables are database tables that store the choices displayed in information field (metadata) lists. Tables and their columns are created using the **Tables** tab of the Configuration Manager. You can have multiple columns in each table but at least two are essential for producing dependent choice lists:

- The common column name used to create the dependency between one list and a second list that is dependent on the choice made from the first (for example, Country and State, respectively).
- The column that stores the choices for metadata lists.

Figure 7-2 Schema Tables Example



Using the geographical example (Country, State, City, Region, Area Code) in the three-tiered schema hierarchy, a table must be created for each *branch* in the schema tree structure. Additionally, the dependent tables (child tables) must contain a column that corresponds to an identical column in the table to which it is subordinate (the parent table). These corresponding columns are used to create the dependencies between the two tables and are ultimately used to generate the dependent choice lists.

For example, the tables in Figure 7-3 illustrate how the Country and State table columns might be populated. The data in each *name* column provides the choices available on the lists. The relationship that is created between the corresponding columns in the Country and State tables (countryID) determines what choices are displayed in the State metadata list.

Figure 7-3 Populated Schema Tables

Country	
countryID	countryName
1	United States
2	Canada

State		
countryID	stateID	stateName
1	1A	Minnesota
1	1B	Wisconsin
2	2A	Manitoba
2	2B	Ontario

7.3.1.2 Views

A view is a tailored presentation of the corresponding table. Views do not contain data, but they derive data from their tables. Views are used to simplify a database for use and to present data in a different perspective.

A view consists of a list of properties and associated display rules. Each table in the schema must have an associated view. Views provide information about these items:

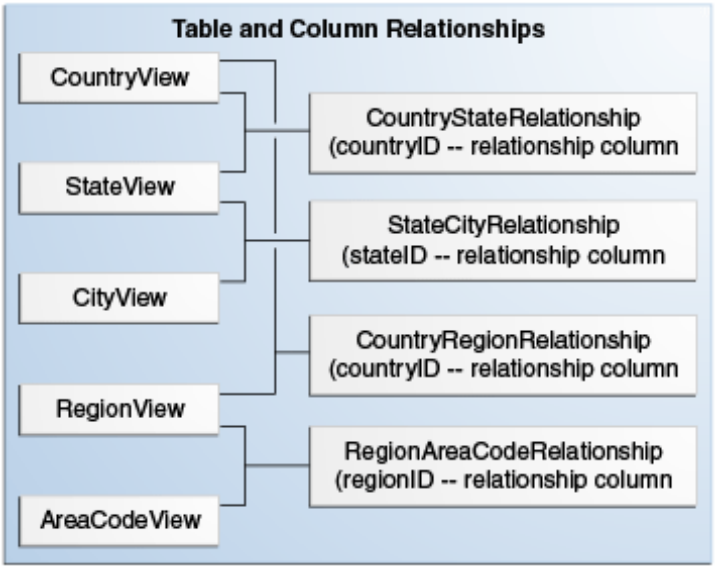
- Specific columns in the table included in the schema. The selected columns are used to establish the dependencies between tables and also to generate the dependent choice lists.
- Internal and external column names.
- User interface display characteristics.
- Editing and sort order criteria.

7.3.1.3 Relationships

Relationships define the dependencies between tables and are essential in generating the appropriate dependent choice lists. Each defined relationship establishes the correspondence between parent and child tables. This correspondence is created by specifying the column in the child table that is dependent on the column in the parent table. Thus, the choices displayed using column data from the child table are contingent on the choice made from the corresponding column data from the parent table.

For example, in Figure 7-4, the CountryView (Country table) and the StateView (State table) use the countryID column to create a relationship that generates a parent country list and a child state list. The choices available in the State metadata list are dependent on the choice made in the Country metadata list.

Figure 7-4 Table and Column Relationships



7.3.1.4 Schema Directory Structure

Three subdirectories are associated with the Schema function, located in the /weblayout/resources directory:

- schema
- schema.work
- schema.old

The schema.work directory is usually not listed because it is a temporary directory. When the schema creation process completes, the working directory is renamed. If this directory exists it indicates one of the following:

- A large schema rebuild is in progress
- The schema is created, but there is a problem with the schema structure.

> **Caution:**
>
> If working inside the directory structure to review the Schema files and directories, be sure to close all open applications accessing these files. The directories are renamed on completion of processing. However, if external applications, such as text editors, are using these files the schema.work directory cannot be renamed.

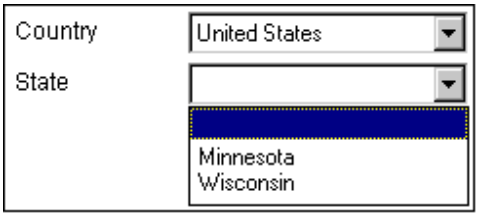
7.3.1.5 Sample Schema-Based Lists

After the schema tables, views, and relationships are created and properly established, the lists display the appropriate choices. For example, in Figure 7-5, the Country list now displays two choices: United States and Canada.

Figure 7-5 List Example

Because the State metadata field is contingent on the Country field, the State list contains items based on the choice made in the Country list. In this case, if the United States choice is selected, the State list displays Minnesota and Wisconsin as choices. If Canada had been selected, then the State list would display Ontario and Quebec.

Figure 7-6 Dependent List Example



7.3.2 Creating Schemas

The **Tables**, **Views**, and **Relations** tabs in the Configuration Manager are used to create the schema structure.

- The **Table** tab is used to select or create the database tables.
- The **Views** tab is used to manipulate the views used in the schema.
- The **Relations** tab is used to manipulate the dependencies.

The **Information Fields** tab is used to create the metadata fields used on Content Server pages. The metadata fields must be correlated to the tables and views to properly display the lists.

New or modified schemas are automatically updated during each scheduled publishing cycle. Because the default interval between each publishing cycle is set to four hours, immediate results for new or modified schemas are not visible. To adjust the interval between each publishing cycle, change the default value of the associated configuration variable. For more information, see Modifying the Publishing Cycle Interval.

This section provides an overview of a simple sequence using the applicable Configuration Manager tabs to create a schema structure.

This section covers the following steps in creating a schema:

- Selecting Tables for the Schema
- Creating the Schema View
- Creating the Schema Relationships

- Adding Metadata Fields
- Enabling the Schema
- Modifying the Publishing Cycle Interval

7.3.2.1 Selecting Tables for the Schema

To select tables for the schema:

1. Use the main menu to choose **Administration** then **Admin Applets**.
2. Click **Configuration Manager** then the **Tables** tab.
3. To add tables to the schema, on the Configuration Manager: **Tables** tab, click **Add Tables** and select the tables to add to the schema from the Select Table page. When creating a new table, click **Create Table**.

> **Important:**
>
> You can use core system tables such as Revisions, Alias, Documents, and Users, but you cannot edit them (remove columns, alter column length, and so on.)

4. On the Create/Edit Table *table_name* page, select the column to be used as a primary key to establish a dependency and select **Edit**.
5. On the Add/Edit Column page, select the box labeled Primary Key and click **OK**. Select **Add Recommended** to add recommended columns to the table.
6. Repeat these steps for all tables to be used in the schema. When finished, click **OK**.

7.3.2.2 Creating the Schema View

To create the schema view:

1. Use the main menu to choose **Administration** then **Admin Applets**.
2. Click **Configuration Manager** then the **Views** tab.
3. To create a view, on the Configuration Manager: **Views** tab, click **Add** to open the Add View page: Select Table page.
4. Select the table to use in the view and click **Next**.
5. On the Add View page: Select Columns page, choose the columns to include in the view, and click **Finish**.
6. On the Add/Edit View page, select a name for the view and add information for the description. Choose the internal column (name in the database) to use in the view and choose the visible column that is displayed to end users. You can specify a display expression (text and Idoc Script) that is displayed in place of the actual field value. When done, click **OK**.
7. Repeat these steps for all tables to be included in the view.

7.3.2.3 Creating the Schema Relationships

To create the schema relationships:

1. After the tables and associated views are completed, click **Relationships** to establish the dependencies between tables and columns. A list of the currently existing schema relationships is displayed.
2. Click **Add** to set up a new schema relation.
3. On the Add/Edit Relationship page, enter the name of the relationship (for example, Country_State to indicate the relationship between the Country and the State tables). In the Parent Info box, select the table where the parent information resides (for example, the Country table) and the column to be used to establish the dependencies (for example, the countryID). Do the same for the Child Info field (for example, select State as the table name and countryID as the relationship).
4. Click **OK** when done.

   The new relationship is now displayed on the **Relations** list.

7.3.2.4 Adding Metadata Fields

The final phase in schema creation is to set up the metadata fields to use the columns and to configure them to use the Views and Relations created previously. For an overview of the procedure, see Adding or Editing a Custom Field and Defining an Option List.

7.3.2.5 Enabling the Schema

After you configure the schema, the views, and the relationships, click the button on the Configuration Manager page to update your database design. Click **Options** then **Publish Schema** from the Configuration Manager page menu.

Republishing (updating) of schema takes place automatically based on these things:

- Existence of the `data/schema/publishlock/publish.dat` file.
- The internal schedule of automatic publishing times. For information about how to modify this schedule, see Modifying the Publishing Cycle Interval.
- How long it took to publish schema last time.

Do not select **Options** then **Publish Schema** unless it is necessary to see the new Content Type quickly. The system can be overloaded when large lists are republished.

7.3.2.6 Modifying the Publishing Cycle Interval

New or modified schemas are automatically updated during the automatic schema publishing cycle. However, by default, the interval between publishing cycles is set to four hours. New schemas or changes to existing schemas are not seen in the corresponding menu lists until the completion of the next publishing cycle. Adjust the publishing cycle interval by changing the value of the SchemaPublishInterval configuration variable.

To change the interval of schema publishing cycles:

1. In a text editor, open the *`IntradocDir`*`/config/config.cfg` file.
2. Add the following configuration variable and value:

   ```
   SchemaPublishInterval=300
   ```

The value is specified in seconds. In this configuration example, the lists are republished every 300 seconds (that is, 5 minutes).

> **Note:**
>
> Depending on the number of lists in addition to the size and complexity of each list, automatically republishing (updating) your schemas frequently can have a significant impact on your system's performance.

3. Save and close the `config.cfg` file.
4. Restart Content Server to apply the changes.

The queries for schema publishing are cached for up to five minutes. Publishing more frequently does not retrieve new values until the current cache expires.

If a new value is added to a metadata field, that value is not displayed on the content item's Content Information page until the next publishing cycle is complete.

If one content item is checked in with a unique value in a dynamic list and a second item is checked in with the same value but using a different case, the value is treated as one value in the list. The case used is dependent on the database sorting scheme.

For more information about creating dynamic lists, see Schema Example: Dynamic Lists.

7.3.3 Schema Example: Dynamic Lists

Creating a *dynamic* list enables users to add values to metadata lists. For example, if a value exists in a list, users can select the value from the list. However, if it is a new value, users can enter the value into a text field and it becomes available as an option following the next publishing cycle.

To create a dynamic list, first create a view into the table in the database. The list values are pulled directly from the metadata columns where they are stored. As content items are checked in, revised, and removed, the list values change or are updated accordingly.

The following steps illustrate an example of creating a dynamic list:

1. Use the main menu to choose **Administration** then **Admin Applets**.
2. Click **Configuration Manager** then the **Information Field** tab.
3. On the Configuration Manager: **Information Field** tab, click **Add**.
4. On the Add Metadata Field Name page, enter the name of the metadata field that has the dynamic list. For example, `TestMetadata`.
5. Click **OK**.
6. On the Add/Edit Metadata Field page, complete the fields as necessary but do not select **Enable Option List**.
7. Click **OK**.

   The page closes and the **Field Info** list on the Configuration Manager: **Information Field** tab shows the added metadata field.
8. Click **Update Database Design**.
9. On the Update Database Design page, click **OK**.

10. Open the Configuration Manager: **Views** tab and click **Add**.
11. On the Add View page: Select Table page, click **Add Table**.
12. On the Select Table page, select the **DocMeta** table.
13. Click **OK**.

    The Select Table page closes and the DocMeta table is added to the Tables list on the Add View page: Select Table page.
14. Click **Next**.
15. On the Add View page: Select Columns page, select the column to use to create the list for TestMetadata.
16. Click **Finish**.
17. On the Add/Edit View page, Enter a view name. For example, `TestMetadata_view`.
18. Click **OK**.
19. Open the Configuration Manager: **Information Fields** tab and select **TestMetadata**.
20. Click **Edit**.
21. On the Add/Edit Metadata Field page, select **Enable Option List**.
22. Click **Configure**.
23. On the Configure Option List page, select **Edit and Select List** from the Option List Type list.
24. Click **Use View** and select a view from the list. For example, `TestMetadata_view`.
25. Click **OK**.
26. On the Configure Option List page, click **OK**.
27. Choose **Publish schema** from the **Options** menu on the Configuration Manager: **Information Field** tab.

Test this list by checking in a document and entering a value into the new dynamic metadata field. Initially, the list is empty because no documents have been checked in that contain data in the TestMetadata field. However, as documents are checked in with values entered in TestMetadata, the list includes the specified values.

7.3.4 Schema Example: Recursive Table for Multiple Trees

Creating a recursive table enables the use of the data for multiple schema trees.

1. Use the main menu to choose **Administration** then **Admin Applets**.
2. Click **Configuration Manager** then the **Information Field** tab.
3. Create a database table with two columns (`id, parent`):
   a. Open the **Tables** tab and click **Create table**.
   b. On the Create/Edit Table *table_name* page, enter the table name. For example, `TreeTest`.
   c. In the Columns pane, click **Add**.
   d. On the Add/Edit Column page, enter the first column name (`id`) and its length. Click **OK**.

e. Enter the second column name (`parent`) and its length. Click **OK**.

f. Click **OK** to create the table.

4. Create a view on the table that includes both columns:

   a. Open the **Views** tab and click **Add**.

   b. In the Tables pane on the Add View page: Select Table page, select `TreeTest` and click **Next**.

   c. In the Columns pane, select the `id` and `parent` check boxes and click **Finish**.

   d. On the Add/Edit View page, enter the view name. For example, `TreeTestView`. Add display, options, and security configurations as applicable.

      Display tab: used to create rules for the relationship.

      Option tab: used to establish the sort order and criteria for the data in the schema.

      Security tab: used to define security rules for the schema.

   e. Click **OK** to create the view.

5. Create a relationship on the view:

   a. Open the **Relations** tab and click **Add**.

   b. On the Add/Edit Relationship page, enter the relationship name. For example, `TreeTestRecursive`.

   c. From the Parent Info table list, select `TreeTest` and in the corresponding column list, select `id`.

   d. From the Child Info table list, select `TreeTest` and in the corresponding column list, select `parent`.

   e. Click **OK** to create the relationship.

6. Open the **Information Fields** tab and click **Add**.

7. On the Add Metadata Field Name page, enter the custom metadata field's name and click **OK**.

8. On the Add/Edit Metadata Field page, select **Enable Option List** and click **Configure**.

9. On the Configure Option List page, click **Use Tree** and click **Edit Definition**.

10. In the Building level pane on the Edit Tree Definition page, select view for level1 list, and select **TreeTestView**.

    TreeTestView is entered as Level 1 in the Tree Definition pane.

11. In the Building level pane: Select relationship between the 1st and 2nd level list, click **TreeTestRecursive**.

    TreeTestRecursive is added under TreeTestView in the Tree Definition pane.

12. In the Building level pane: Select view for level 2 list, click **TreeTestView (recursive to level 1)**.

    TreeTestView (recursive to level 1) is entered as Level 2 in the Tree Definition pane and the **Select root** button is added.

13. Click **Select root**.

    The Select Tree Root dialog opens.

8
Categorizing and Linking Content

This chapter provides information about how to categorize and link content using Oracle WebCenter Content Server components Content Categorizer and Link Manager.

- About Categorizing and Linking Content
- Categorizing Content
- Using the Link Manager Component

8.1 About Categorizing and Linking Content

Content Categorizer and Link Manager are optional components automatically installed with Oracle WebCenter Content Server. When enabled, Content Categorizer suggests metadata values for new documents checked in to Content Server, and for existing documents that have or do not have metadata values. When Link Manager is enabled, it evaluates, filters, and parses the URL links of indexed content items before extracting them for storage in a database table (ManagedLinks).

8.2 Categorizing Content

For Content Categorizer to recognize structural properties, the content must go through XML Conversion (eXtensible Markup Language). The conversion method is defined in the `sccXMLConversion` configuration variable. Content Categorizer uses Search Rules to suggest metadata values for content:

The Batch Categorizer that is included with the component can search a large number of files and create a Batch Loader control file containing appropriate metadata field values. The Batch Categorizer can also be used to recategorize content checked in to the repository.

- XML Conversion
- Search Rules Overview
- Running Content Categorizer

8.2.1 XML Conversion

> **Important:**
>
> There is a problem with the XSLT transformation used to post-process PDF content converted using the Flexiondoc schema. When Flexiondoc schema are used, single words are assigned to individual XML elements, making the final XML unusable. It is necessary to use SearchML for categorizing PDF content.

Regardless of which XML converter is specified, the XML intermediate files are used only by Content Categorizer, so they are discarded after use, and documents are checked in to

Content Server in their original source form. The only exception is content that is in XML format, which is not subjected to the translation process.

With each converter, the OutsideIn XML Export technology is used in combination with a custom XSLT style sheet (`flexiondoc_to_scc.xsl`) to produce XML in a two-stage process. In the first stage, the native document is converted to either Flexiondoc-formatted XML or SearchML-formatted XML.

In the second stage, the style sheet is used to further refine the XML so that it is searchable by Content Categorizer. Native document properties and text segments are isolated in XML elements, which are named after the corresponding document property, paragraph style, or character style (note that character styles are not supported by SearchML).

For a list of file formats supported by OutsideIn XML Export, see Input File Formats.

8.2.2 Search Rules Overview

Content Categorizer executes search rules depending on the type of rule defined:

- Pattern Matching and Abstract Rules: Content Categorizer scans a content document looking for "landmarks." A landmark can be specific text, or it can be based on structural properties of the source document, such as styles, fonts, and formatting.
- Option List Rule: Content Categorizer searches for keywords whose cumulative score determines which option of a list is selected. It does not look for either landmarks or specific XML tags.
- Categorization Engine Rule: Content Categorizer invokes a 3rd-party categorizer engine and taxonomy to categorize a content item.
- Filetype Rule: Content Categorizer looks for the document file type (the file name extension).

Normally, a user-entered value on the Content Check In Form prevents Content Categorizer from applying the search rules for that field. This is also true for list fields that have a default value, such as the Type field.

> **Important:**
>
> It is important to instruct contributors to leave any fields blank that they want to have filled by search rules.

For more information about search rules, see Search Rules.

8.2.3 Running Content Categorizer

The following tasks must be done to run Content Categorizer:

- Define the XML Conversion method. For more information, see Setting XML Conversion Method.
- Define search rules. For more information, see Creating Search Rules.

- Optional: Define field properties, including default values for metadata fields. For more information, see Defining Field Properties (Optional).

> **Important:**
>
> To use the CATEGORY search rule, install, set up and register a categorizer engine before defining the CATEGORY rule for any metadata fields.

8.2.3.1 Operating Modes

Content Categorizer can operate in either Interactive mode or Batch mode. All modes require conversion of the source documents into XML intermediate form. However, the process flows of the modes are distinctly different.

- **Batch** mode is used when recategorizing large numbers of documents in the repository. The system administrator uses a standalone utility to run Content Categorizer, then either performs a live update of content metadata or uses the output file from Batch Categorizer as input to the Batch Loader. For more information about the steps used during this process, see Running Batch Mode.
- **Interactive** mode integrates Content Categorizer with the Content Check In Form and Info Update Form. Users click **Categorize** on the form to run Content Categorizer on a single content item. Any value that is returned by Content Categorizer is a suggested value, because the contributor can edit or replace the returned value. For more information about the steps taken during this process, see Interactive Mode Process.

8.2.3.1.1 Running Batch Mode

The `MaxQueryRows` configuration variable is used to specify the maximum number of documents that can be included in a single batch load process. As such, it affects how many documents a user sees in Batch Categorizer. The default setting for this configuration variable is 200 but can be decreased or increased as necessary. For more information about the variable, see *Configuration Reference for Oracle WebCenter Content*.

The system administrator performs the following steps during the batch mode process:

1. Run the Batch Categorizer application. For more information about running applications on UNIX systems, see *Administering Oracle WebCenter Content*.
2. If necessary, on the Batch Categorizer page, define filters and release date information to display a list of content to be categorized. Click **Categorize**.
3. On the Categorize Existing page, select **Live Update** or **Batch Loader**.
   - The Live Update option updates the data in the repository immediately.
   - The Batch Loader option is used to create a control file, which is the output of the Content Categorizer process. The file contains an entry for each source document, and contains the values for each metadata field based on the search rules defined in Content Categorizer. You can edit this file before submitting it to the Batch Loader.
4. To run the Batch Loader utility automatically after the Content Categorizer process is complete, select the **Run Batch Loader** check box.
5. Enter the location and file name for the log file that contains error information about the Content Categorizer process.

6. Choose **Categorize All** to work with all content items or **Categorize Selected** to use only the highlighted items in the content list.
7. Choose to categorize the **Latest Revision**, which works with only the most recent revision of an item, or **All Revisions**.
8. Choose to continue or discontinue the categorization process when Batch Categorizer encounters an error.
9. Click **OK**. The Progress bar shows the progress as the batch process moves through its steps:
    a. Content Categorizer locates the source content.
    b. If the content is in XML format, no translation occurs, and the process continues at step d.
    c. If the content is not in XML format, conversion into XML occurs using the selected XML conversion method: Flexiondoc or SearchML.
    d. Content Categorizer applies the search rules to the XML and obtains values for the specified metadata fields.
    e. If Live Update was specified, database records are updated immediately. If Batch Loader was specified, an output control file is created, and the Batch Loader utility is run, if the option to do so after processing was specified.
10. When the batch process is complete, review the error logs. Errors encountered by Batch Categorizer are displayed on the console and also recorded in the Batch Categorizer log (if specified). Errors encountered by Batch Loader are displayed on the console and also recorded in the system log.

If the optional AddCCToArchiveCheckin component is installed and enabled, all content loaded using the Batchloader utility is categorized automatically, based on predefined rule sets. For more information about defining rule sets, see Creating Search Rules.

8.2.3.1.2 Interactive Mode Process

The following steps occur during the check-in process:

1. A contributor opens the Content Check In Form or the Info Update Form, selects a primary file (only on Content Check In Form), and clicks **Categorize**.
2. The Content Check In Form copies the primary file to the host and calls the Content Categorizer service.
3. Content Categorizer locates the source content.
4. If the content is in XML format, no translation occurs, and the process continues at step 6.
5. If the content is not in XML format, the specified conversion method is used.
6. Content Categorizer applies the search rules to the XML and obtains suggested values for the specified metadata fields.
7. Content Categorizer inserts the suggested metadata values into the Content Check In Form or Update Info Form, and returns the form to the contributor.
8. The contributor can check in or submit the document with the suggested values, revise the metadata values, or cancel the check in or update.

If the optional AddCCToNewCheckin component is installed and enabled, when you click **Check In** on the Content Check In Form, it performs steps 2 through 6 and completes the check in process, provided the properties for dDocTitle are set to **Override Contents**.

If the properties of dDocTitle are not set to Override Contents, then an alert is displayed requesting that the required field is completed. Field properties are set using the Content Categorizer admin applet. For more information, see Defining Field Properties (Optional).

8.2.4 Setting Up Content Categorizer

Before using Content Categorizer, install and configure the necessary software. This section discusses those tasks:

- Setting XML Conversion Method
- Defining Field Properties (Optional)

8.2.4.1 Setting XML Conversion Method

To set the XML conversion method in Content Categorizer:

1. Use the main menu to choose **Administration** then **Content Categorizer Administration**.
2. On the Content Categorizer Administration page, click **Configuration**.
3. On the **Configuration** tab, select the **sccXMLConversion** property and click **Edit** or double-click the property.
4. From the list on the Property Config page, select either **Flexiondoc** or **SearchML** as the XML conversion method.
5. Click **OK**.
6. Click **Apply** to save the changes.

8.2.4.2 Defining Field Properties (Optional)

When any rule for a field succeeds, the found value is used (in either Batch Loader operations or Live Update operations). However, depending on how the Override value is set, the found value does not override the existing value (Override is set to false).

When all rules for a field fail, no value is assigned to the field unless a default value is defined for the field and Use Default is set to true.

To define field properties for the metadata fields:

1. Use the main menu to choose **Administration** then **Content Categorizer Administration**.
2. On the Content Categorizer Administration page, click the **Field Properties** tab.
3. Select a metadata field to be edited and click **Edit**, or double-click the field.
4. On the Field Properties page, enter a default value for the field. The default value for a list field must match a value available for that field.
5. Select the Override check box for the value returned by the categorization process to override an existing value for the field.
6. Select the Use Default check box for the field's default value to be used if all rules fail (or are not defined) when the categorization process runs.

7. Click **OK**.
8. Repeat these steps for each field to be edited.
9. Click **Save Settings** to save the changes.

8.2.5 Search Rules

Search rules define how Content Categorizer determines metadata values to return to the Content Check In Form or Info Update Form (for Interactive mode) or the batch file (for Batch mode).

This section discusses the following information regarding search rules:

- Pattern Matching Search Rules
- Abstract Search Rules
- Option List Search Rule
- Categorization Engine Search Rule
- Filetype Search Rule
- Creating Search Rules

Every search rule is defined by:

- A **rule type**, which determines the method that Content Categorizer uses to search the XML document.
- A **key**, which defines the XML element, phrase, or keyword that Content Categorizer looks for in the document, or the categorization engine/taxonomy that Content Categorizer uses to classify the document.
- A **count**, which is used to refine the search criteria.

Consider the following guidelines when creating search rules:

- You can apply search rules to any custom metadata field.
- You can apply search rules to the Title, Comments, and Type standard metadata fields. You cannot define search rules for any other standard metadata fields (such as Author, Security Group, and Account).
- You can define multiple search rules for a metadata field. (For a single metadata field, however, multiple CATEGORY rules referring to different taxonomies are not supported.)
- Multiple search rules are run in the order specified, so that if a search rule does not result in a suggested value, the next rule is run. Arrange the list from most to least specific.
- You can mix search rule types within a metadata field. For example, you can define an Option List rule, a Pattern Matching rule, and an Abstract rule for the same metadata field.
- If none of the search rules specified for a metadata field can be satisfied, the field is left blank.

8.2.5.1 Pattern Matching Search Rules

Pattern Matching search rules look for specific text or a specific XML element and return an associated value. For example, the *Invoice* #metadata field contain the value

that follows an *Invoice:* or *Invoice Number:* label in the source document, or it can contain the value that is within the <*Invoice*> tag in the XML document.

There are two general types of Pattern Matching rules: Tag Search and Text Search. Within each type are several sub-types.

- Tag Search searches for the full name of an XML element that matches the key. If such an element is found, the text contained in the element is returned as the result. Tag searches are case sensitive. Sub-types include the following:
  - TAG_TEXT
  - TAG_ALLTEXT
- Text Search searches for text that matches the key. If such text is found, the text near or following the key is returned as the result. Text searches are not case sensitive. Sub-types include the following:
  - TEXT_REMAINDER
  - TEXT_FULL
  - TEXT_ALLREMAINDER
  - TEXT_ALLFULL
  - TEXT_NEXT
  - TEXT_ALLNEXT

The *key* for a Pattern Matching search rule is either an XML element (for a Tag Search) or a text phrase (for a Text Search).

The *count* for a Pattern Matching search rule defines the number of tags or text phrases that must be matched before the rule returns results. For example, a count of 4 looks for the fourth occurrence of the key. If only three occurrences of the key are found in the document, the rule fails.The default count of 1 returns the first occurrence of the key.

The following examples illustrate the use of the Pattern Matching search rules.

Example: TAG_TEXT

This rule searches for the full name of an XML element that matches the key (including case). If such an element is found, all text that belongs to the element is concatenated and returned as the result.

- **Content:** <TAG_A>Title: The Big <TAG_B>Bad</TAG_B> Wolf</TAG_A>

  <TAG_C>Subtitle: A <TAG_D>Morality</TAG_D> Play</TAG_C>
- **Rule:** TAG_TEXT
- **Key:** TAG_A
- **Returns:** Title: The Big Wolf

Example: TAG_ALLTEXT

This rule searches for the full name of an XML element that matches the key (including case). If such an element is found, all text that belongs to the element, and to all children of the element, is concatenated and returned as the result.

- **Content:** <TAG_A>Title: The Big <TAG_B>Bad</TAG_B> Wolf</TAG_A>

  <TAG_C>Subtitle: A <TAG_D>Morality</TAG_D> Play</TAG_C>

- **Rule:** TAG_ALLTEXT
- **Key:** TAG_A
- **Returns:** Title: The Big Bad Wolf

Example: TEXT_REMAINDER

This rule searches for text that matches the key (except for case). If such text is found, any text following the key that belongs to the same XML element is returned as the result.

- **Content:** <TAG_A>Title: The Big <TAG_B>Bad</TAG_B> Wolf</TAG_A>

  TAG_C>Subtitle: A <TAG_D>Morality</TAG_D> Play</TAG_C>
- **Rule:** TEXT_REMAINDER
- **Key:** Title:
- **Returns:** The Big Wolf

Example: TEXT_ALLREMAINDER

This rule searches for text that matches the key (except for case). If such text is found, any text following the key that belongs to the same XML element, and to all children of the element, is returned as the result.

- **Content:** TAG_A>Title: The Big <TAG_B>Bad</TAG_B> Wolf</TAG_A>

  <TAG_C>Subtitle: A <TAG_D>Morality</TAG_D> Play</TAG_C>
- **Rule:** TEXT_ALLREMAINDER
- **Key:** Title:
- **Returns:** The Big Bad Wolf

Example: TEXT_FULL

This rule searches for text that matches the key (except for case). If such text is found, any text that belongs to the same XML element, including the key text, is returned as the result.

- **Content:** <TAG_A>Title: The Big <TAG_B>Bad</TAG_B> Wolf</TAG_A>

  <TAG_C>Subtitle: A <TAG_D>Morality</TAG_D> Play</TAG_C>
- **Rule:** TEXT_FULL
- **Key:** Title:
- **Returns:** Title: The Big Wolf

Example: TEXT_ALLFULL

This rule searches for text that matches the key (except for case). If such text is found, any text that belongs to the same XML element, including the key text and any text belonging to children of the element, is returned as the result.

- **Content:** <TAG_A>Title: The Big <TAG_B>Bad</TAG_B> Wolf</TAG_A>

  <TAG_C>Subtitle: A <TAG_D>Morality</TAG_D> Play</TAG_C>
- **Rule:** TEXT_ALLFULL

- **Key:** Title:
- **Returns:** Title: The Big Bad Wolf

Example: TEXT_NEXT

This rule searches for text that matches the key (except for case). If such text is found, any text that belongs to the next non-blank XML element is returned as the result. Blank elements and elements composed of non-printing characters are not selected as the return value.

- **Content:** <TAG_A>Title: The Big <TAG_B>Bad</TAG_B> Wolf</TAG_A>

  <TAG_C>Subtitle: A <TAG_D>Morality</TAG_D> Play</TAG_C>
- **Rule:** TEXT_NEXT
- **Key:** Title:
- **Returns:** Subtitle: A Play

Example: TEXT_ALLNEXT

This rule searches for text that matches the key (except for case). If such text is found, any text that belongs to the next non-blank XML element, and to all children of the element, is returned as the result. Blank elements and elements composed of non-printing characters are not selected as the return value.

- **Content:** <TAG_A>Title: The Big <TAG_B>Bad</TAG_B> Wolf</TAG_A>

  <TAG_C>Subtitle: A <TAG_D>Morality</TAG_D> Play</TAG_C>
- **Rule:** TEXT_ALLNEXT
- **Key:** Title:
- **Returns:** Subtitle: A Morality Play

8.2.5.2 Abstract Search Rules

Abstract search rules look for an XML element and return a descriptive sentence or paragraph from that element. For example, the *Summary* metadata field could be filled by a returned value of "Germany is a large country in size, culture, and worldwide economics. One of Germany's largest industries includes the manufacturing of world class automobiles like BMW, Mercedes, and Audi."

The Abstract rule type is useful where there is no readily identifiable or explicitly tagged block of text in the content item. Typically, these rules are used to suggest summary or topic information about the document.

There are two *types* of abstract search rules: First Paragraph and First Sentence.

- First Paragraph searches for the full name of an XML element that matches the key. The entire paragraph of the first such element that meets the size criteria (specified by the count) is returned as the result.
- First Sentence searches for the full name of an XML element that matches the key. If such an element is found, the first sentence of the element is returned as the result.

The *key* for an Abstract search rule is an XML element.

The *count* is interpreted differently for the First Paragraph and First Sentence search rules.

- For a First Paragraph search rule, the count is a size threshold measured in percent:

1. The rule searches the document for all paragraphs that match the key.
2. The rule calculates the average size (based on character count) of the paragraphs that match the key.
3. The rule multiplies the average size by the count percentage (0 =0%, 100 =100%).
4. The rule looks for the first paragraph larger than the resulting number.

   For example, if the count is set to 75 and the average paragraph size is 100 characters, the rule returns the first paragraph larger than 75 characters that matches the key.

   If the count is set to the default of 1, the rule is likely to return the first paragraph that matches the key.

- For a First Sentence search rule, the count is the number of elements that have their first sentences returned.

  For example, if the count is set to 3, the rule returns the first sentence from each of the first three elements that match the key.

The following examples illustrate the use of the Abstract search rules.

Example: FIRST_PARAGRAPH

This example returns the first <Text> element that exceeds one-half the average <Text> element paragraph size. Note that the <Title> element does not match the key value, so it is ignored for both the search and for the average length calculation.

- **Content:** <Title>Poem</Title>

  <Text>Mary had</Text>

  <Text>a little Lamb</Text>

  <Text>The fleece was white as snow</Text>

  <Text>And everywhere that Mary went the lamb was sure to go</Text>
- **Rule:** FIRST_PARAGRAPH
- **Key:** Text
- **Count:** 50
- **Returns:** The fleece was white as snow.

Example: FIRST_SENTENCE

This example returns the first sentence of the first two <Text> elements. Note that the<Title> element does not match the key value, so it is excluded from the search.

- **Content:** x<Title>Barefoot in the Park</Title>

  <Text>See Dick run. See Jane run. See Dick and Jane.</Text>

  <Text>See Spot run. See Puff chase Spot.</Text>

  <Text>See Dick chase Spot and Puff.</Text>
- **Rule:** FIRST_SENTENCE
- **Key:** Text
- **Count:** 2

- **Returns:** See Dick run. See Spot run.

8.2.5.3 Option List Search Rule

The Option List search rule looks for keywords within the source document, applies a score for each keyword found, and returns the value that has the highest keyword score.

For example, if the keywords *margin*, *SEC filing*, or *invoice* were found in a document, the suggested value for the *Department* field would be *Accounting*, while the keywords *tolerance*, *assembly*, or *inventory* would return *Manufacturing* as the suggested value.

- The Option List search rule usually applies to metadata fields that have a list defined in the Configuration Manager.
- Option list names and values (called **categories** in Content Categorizer) appear in Content Categorizer as specified in the Configuration Manager. If a custom list field is created or changed while the CC Admin Applet is open, close and reopen the applet to see the changes.
- The current version of Content Server automatically inserts a blank value as the default value in a custom list field. In this case, the first value (by default, a blank value) is not considered a user-entered value, and the Option List search rule is applied. To prevent the Option List search rule from overriding the first value in a custom list field, provide a default value for that list on the Configuration Manager Applet.

There is one *type* of Option List search rule, which searches for keywords (single words or phrases) that match the keywords defined in the key.

- Keywords can be single words (for example, *dog*) or multiple-word phrases (for example, *black dog*).
- Keywords can use the following defined set of operators to further refine a search:
  - $$AND$$
  - $$OR$$
  - $$AND_NOT$$
  - $$NEAR$$
- Keywords are pre-assigned to each category (value) in the list, and each keyword has a weight assigned to it.
- The number of occurrences of each keyword found in the document is multiplied by its weight, resulting in a keyword score.
- The keyword scores for each category are added, resulting in a category score.
- The category with the highest score is returned as the suggested value.
- If there is a tie between categories, the category earliest in the list is returned as the suggested value.
- Use the weights *Always* and *Never* to override the scores and count threshold.
  - An occurrence of a keyword with the *Always* weight forces the category to be returned as the suggested value, regardless of score.
  - An occurrence of a keyword with the Never weight disqualifies the category from being returned as the suggested value, regardless of score.
  - If two categories have keywords assigned the *Always* weight, and both keywords occur in the document, the keyword first found in the document takes precedence.

> **Important:**
>
> Option List searches are case sensitive and must match exactly. For example, *Invoice*, *Invoices*, *invoice*, and *invoices* must be defined to retrieve all instances of this keyword.

The *key* for an Option List search rule is the Option List name, as shown on the **Option Lists** tab of the Admin Applet.

The *count* for an Option List search rule sets a minimum threshold score for the rule to return results. For example, if the count is set to 50, and the highest accumulated keyword score is 45, the rule fails.

The following examples illustrate the use of the Option List search rule.

Example 1: Option List

In this example, the score for *Dick* and *Spot* is 30 (3 occurrences x 10), and the score for *Jane* and *Puff* is 20 (2 occurrences x 10). *Dick* is returned as the suggested value because it is earlier in the list than *Spot*:

- **Content:** <Title>Barefoot in the Park</Title>

  <Text>See Dick run. See Jane run. See Dick and Jane.</Text>

  <Text>See Spot run. See Puff chase Spot.</Text>

  <Text>See Dick chase Spot and Puff.</Text>
- **Rule:** OPTION_LIST
- **Key:** MainCharacterList
- **Count:** 10
- **Option List Categories, Keywords, and Weight:** Dick: Dick=10, boy=5, Richard=2

  Jane: Jane=10, girl=5, Janie=2

  Spot: Spot=10, dog=5

  Puff: Puff=10, cat=5
- **Returns:** Dick

Example 2: Option List

In this example, *Spot* is returned as the suggested value because its score of 60 (3 occurrences x 20) is higher than the other categories:

- **Content:** <Title>Barefoot in the Park</Title>

  <Text>See Dick run. See Jane run. See Dick and Jane.</Text>

  <Text>See Spot run. See Puff chase Spot.</Text>

  <Text>See Dick chase Spot and Puff.</Text>
- **Rule:** OPTION_LIST
- **Key:** MainCharacterList
- **Count:** 10

- **Option List Categories, Keywords, and Weight:** Dick: Dick=10, boy=5, Richard=2

  Jane: Jane=10, girl=5, Janie=2

  Spot: Spot=20, dog=10

  Puff: Puff=10, cat=5
- **Returns:** Spot

Example 3: Option List

In this example, the rule fails because none of the scores is above the Count threshold of 50:

- **Content:** <Title>Barefoot in the Park</Title>

  <Text>See Dick run. See Jane run. See Dick and Jane.</Text>

  <Text>See Spot run. See Puff chase Spot.</Text>

  <Text>See Dick chase Spot and Puff.</Text>
- **Rule:** OPTION_LIST
- **Key:** MainCharacterList
- **Count:** 50
- **Option List Categories, Keywords, and Weight:** Dick: Dick=10, boy=5, Richard=2

  Jane: Jane=10, girl=5, Janie=2

  Spot: Spot=10, dog=5

  Puff: Puff=10, cat=5
- **Returns:** Fail

Example 4: Option List

In this example, *Puff* is returned as the suggested value because the keyword "Puff" has a weight of Always:

- **Content:** <Title>Barefoot in the Park</Title>

  <Text>See Dick run. See Jane run. See Dick and Jane.</Text>

  <Text>See Spot run. See Puff chase Spot.</Text>

  <Text>See Dick chase Spot and Puff.</Text>
- **Rule:** OPTION_LIST
- **Key:** MainCharacterList
- **Count:** 10
- **Option List Categories, Keywords, and Weight:** Dick: Dick=10, boy=5, Richard=2

  Jane: Jane=10, girl=5, Janie=2

  Spot: Spot=10, dog=5

  Puff: Puff=Always, cat=5
- **Returns:** Puff

8.2.5.4 Categorization Engine Search Rule

The Categorization Engine search rule uses a third-party categorizer engine and defined taxonomy to determine and return a value that represents a category within the specified taxonomy, for example, News/Technology/Computers.

There is one *type* of Categorization Engine search rule, which uses the categorizer engine and taxonomy specified in the Key to return a value for the field.

The *key* for a Categorization Engine search rule is the name of the categorizer engine followed by the name of the taxonomy. For example, *EngineName/TaxonomyName*. If an engine name is defined in the Key field, Content Categorizer defaults to the first engine displayed in the Categorizer Engines list. If only one engine is defined, just enter the taxonomy name in the Key field.

The *count* for a Categorization Engine search rule sets a minimum confidence level threshold for the returned results.

When a categorization engine returns a category (or set of categories) for a given query, a confidence level is also returned, which is often expressed as a percentage for each category. The Category rule always accepts the highest-confidence category, **unless** the confidence level is below the count value specified for the rule, in which case the rule fails. For example, if the count is set to 50, and the highest-confidence category returned is 45, the rule fails.

The default count of 1 would always accept the highest-confidence category returned by the categorizer engine. The actual range for the Count value depends on the categorizer engine that is being used.

8.2.5.5 Filetype Search Rule

The Filetype search rule looks at the file name extension of a document and returns a term, usually a file type description associated with the file name extension.

There is one *type* of Filetype search rule, which uses the file name extension of the primary (native) file to return a value for the field.

When the Filetype search rule is defined for a metadata field, the file name extension of the content item is matched against all values in the DocFormatsWizard table. This table is found in the file `doc_config.htm`, which is located in the *`IntradocDir`*`/shared/config/resources/` directory.

If a match is found, the associated value in the Description column is extracted and translated. The resulting string is returned as the suggested metadata value for the field. If the primary file path has no extension, or if the extension does not match any of the "extensions" values in the DocFormatsWizard table, the rule fails and the next rule in the list for the metadata field is executed.

The *key* for a FILETYPE search rule is not used when determining a metadata value. **Leave the Key field blank.**

The count for a FILETYPE search rule is not used when determining a metadata value. **Leave the Count field blank.**

If a FILETYPE rule is created with non-blank Key or Count fields, a warning message is displayed indicating that these fields are not supported by the rule.

The following examples illustrate the use of the Filetype Search rule.

Example 1: Filetype Search

- **Primary File:** policies.doc
- **Rule:** FILETYPE
- **Key:** blank
- **Count:** blank
- **Returns:** Microsoft Word Document

Example 2: Filetype Search

- **Primary File:** procedures.wpd
- **Rule:** FILETYPE
- **Key:** blank
- **Count:** blank
- **Returns:** Corel WordPerfect Document

8.2.5.6 Creating Search Rules

During startup, Content Categorizer takes a snapshot of the current metadata field configuration including field names and lengths. If the metadata field configuration changes, restart Content Server before running the Content Categorizer Admin Applet to add or modify any search rules.

> **Important:**
>
> Content Categorizer requires a non-empty rule set for any file type (`.doc`, `.txt`, `.xml`, and so on) it is called to examine. If no rules exist for a given file type, Content Categorizer throws an exception.The easiest way to protect against this is to add at least one rule to the Default rule set. The Default rule set is used for all file types which do not have a custom rule set assigned.

To define search rules for any metadata field:

1. Use the main menu to choose **Administration** then **Content Categorizer Administration**.
2. On the Content Categorizer Administration page, click the **Rule Sets** tab.
3. In the Ruleset pane, select the ruleset from the list, or click **Add** to add and name a new ruleset. A ruleset contains multiple rules that apply to specific documents or a particular document type. If a specific ruleset is not defined for a given document or document type, the default ruleset is used.
4. Select a metadata field from the **Field** list.
5. Click **Add**.
6. On the Add/Edit Rule for *field_name* page, select the rule type from the **Rule** list.
7. Enter the search rule key in the **Key** field.

If CATEGORY is used, enter the categorization engine name (if there are multiple items in list of Categorizer Engines), followed by slash (/), followed by taxonomy name. For example: *EngineName/TaxonomyName*

For an OPTION_LIST search rule, keywords for the list must be defined on the **Option List** tab.

8. Enter the count in the **Count** field. For TAG and TEXT types, this is the number of tags or text phrases that must be matched before the rule returns results. For example, a count of 4 looks for the fourth occurrence of the key.

   If only three occurrences of the key are found in the document, the rule fails. The default count of 1 returns the first occurrence of the key.

   For FIRST_PARAGRAPH, this is the size threshold measured in percent. The first paragraph matching the key that is larger than the count percentage multiplied by the average paragraph size is returned. For example, if the count is set to 75 and the average paragraph size is 100 characters, the rule returns the first paragraph larger than 75 characters that matches the key. If the count is set to the default of 1, the rule is likely to return the first paragraph that matches the key.

   For FIRST_SENTENCE, this is the number of elements that have their first sentences returned. For example, if the count is set to 3, the rule returns the first sentence from each of the first three elements that match the key.

   For CATEGORY, this is the minimum confidence level threshold for the rule to return results. For example, if the count is set to 50, and the highest-confidence category has a confidence level of 45, the rule fails.

9. Click **OK** when done.

10. Add search rules to each metadata field as necessary.

    - To delete a rule, select the rule in the **Rules List** and click **Delete**.
    - To edit a rule, select the rule in the **Rules List** and click **Edit**.
    - To adjust the order of the rules, select the rule in the **Rules List** and click **Move Up** or **Move Down**. Rules are applied in the order listed. If the first rule succeeds, no other rules are applied. If the first rule fails, then the next rule is applied, and so forth.

    > **Important:**
    >
    > If a CATEGORY rule is added, edited, or deleted, a dialog prompts you to apply the changes and build, rebuild, or check for orphaned query trees for this rule on the **Query Trees** tab.

11. Click **Apply** to save the changes, or click **OK** to save the changes and close the Content Categorizer Administration page.

8.2.5.6.1 Defining keywords and weights for a list

To define keywords and weights for a list:

1. Use the main menu to choose **Administration** then **Content Categorizer Administration**.
2. On the Content Categorizer Administration page, click the **Option Lists** tab.

3. Select a list from the **Option List**. The list includes the Type ($DocType) list, plus lists of all custom metadata fields that have a list defined in the Configuration Manager.

> **Caution:**
>
> When a list metadata field is deleted from the Configuration Manager, the field is removed from the **Rule Sets** tab, but it still appears in the Option List list on the **Option Lists** tab. Be careful not to select an obsolete list.

4. Select a value from the Category list. Only the pre-defined values for the list are included.
5. Enter a keyword or phrase in the Keyword field. Option List searches are case sensitive and must match exactly.
   - Keywords can be single words or multiple-word phrases.
   - Keywords can include Boolean-type expressions, where the following set of binary operators are valid: $$AND$$, $$OR$$, $$AND_NOT$$, $$NEAR$$
6. Select a weight for the keyword.
   - Always: If the keyword is found, the selected category is returned as the suggested value, regardless of the score.
   - Weight: This number multiplied by the number of occurrences of the keyword is the category's score. The category with the highest score is returned as the suggested value for the list field.
   - Never: If the keyword is found, the selected category is not returned as the suggested value, regardless of the score.
7. Click **Add**.
8. Enter keywords for each category in the selected list.
   - To delete a keyword, select the keyword in the Keywords list and click **Delete**.
   - To edit a keyword, select the keyword in the Keywords list, click **Edit**, edit the keyword, the weight or both, and click **Update**.
9. Click **Apply** to save the changes, or click **OK** to save the changes and close the page.

You can configure the configuration file so Content Categorizer ignores the **Type** default value and applies search rules to the **Type** field.

This procedure applies only to the **Type** (dDocType) field. You cannot apply search rules to the other standard list fields (Security Group, Author, and Account).

8.2.5.6.2 Applying search rules to the Type field

To apply search rules to the Type field:

1. Open the `config.cfg` file located in the *`IntradocDir`*`/config/` directory using a text-only editor such as WordPad.
2. Add the following line to the file:

   ```
   ForceDocTypeChoice=true
   ```

3. Save and close the file.
4. Stop and restart Content Server.

8.2.6 Sample doc_config.htm Page

The following is a sample `doc_config.htm` page.

```
<@table DocFormatsWizard@>
```

dFormat	Extensions	dConversion	dDescription
application/ corel-wordperfect, application/ wordperfect	wpd	WordPerfect	apWordPerfectDesc
application/ vnd.framemaker	fm	FrameMaker	apFramemakerDesc
application/ vnd.framebook	bk, book	FrameMaker	apFrameMakerDesc
application/vnd.mif	mif	FrameMaker	apFrameMakerInterchangeDesc
application/lotus-1-2-3	123, wk3, wk4	123	apLotus123Desc
application/lotus-freelance	prz	Freelance	apLotusFreelanceDesc
application/lotus-wordpro	lwp	WordPro	apLotusWordProDesc
application/msword, application/ms-word	doc, dot	Word	apMicrosoftWordDesc
application/vnd.ms-excel, application/ms-excel	xls	Excel	apMicrosoftExcelDesc
application/ vnd.ms-powerpoint, application/ms-powerpoint	ppt	PowerPoint	apMicrosoftPowerPointDesc
application/vnd.ms-project, application/ms-project	mpp	MSProject	apMicrosoftProjectDesc
application/ms-publisher	pub	MSPub	apMicrosoftPublisherDesc
application/write	wri	Word	apMicrosoftWriteDesc
application/rtf	rtf	Word	apRtfDesc
application/vnd.visio	vsd	Visio	apVisioDesc
application/vnd.illustrator	ai	Illustrator	apIllustratorDesc
application/vnd.photoshop	psd	PhotoShop	apPhotoshopDesc
application/vnd.pagemaker	p65	PageMaker	apPageMakerDesc
image/gif	drw, igx, flo, abc, igt	iGrafx	apiGrafxDesc
text/postscript	ps	Distiller	apDistillerDesc
application/hangul	hwp	Hangul97	apHangul97Desc
application/ichitaro	jtd, jtt	Ichitaro	apIchitaroDesc

dFormat	Extensions	dConversion	dDescription
image/graphic	gif, jpeg, jpg, png, bmp, tiff, tif	ImageThumbnail	apThumbnailsDesc
image/application	txt, eml, msg	NativeThumbnail	apNativeThumbnailsDesc

```
<@end@>
<@table PdfConversions@>
```

dFormat	Extensions	dConversion	dDescription
application/pdf	pdf	PDFOptimization	apPdfOptimization
application/pdf	pdf	ImageThumbnail	apPdfThumbnailsDesc

```
<@end@>
```

8.2.7 XSLT Transformation

Content Server uses a two-step process for categorizing content. The first step translates content into an XML format, the second step transforms the XML file into another XML file useful to Content Categorizer. The process is transparent in that the original content is not modified, and both the translated and transformed XML files are discarded after use.

This section covers the following topics:

- Translation
- Transformation Using XSLT Style Sheets
- SearchML Transformation
- Flexiondoc Transformation

8.2.7.1 Translation

The translation step uses the OutsideIn XML Export filters to output the XML in either SearchML or Flexiondoc XML format, depending on the type of content being translated and if the format is available for the platform being used. This translation process enables Categorizer to support a large number of different source document formats.

The transformation step uses eXtensible Style Sheet Language Transformations (XSLT) to transform the initial XML output into an XML equivalent that Content Categorizer can easily search and analyze based on search rules defined by the user.

An overview of the transformation process can be useful to anyone interested in the categorization process, and serve as a starting point for users who would like to define their own XSLT style sheets to accommodate their specific document processing needs.

Translation Using OutsideIn XML Export Filters

A run-time version of the OutsideIn XML Export product is integrated and installed with Content Server, and it filters content checked in for categorization. The Export filters convert content to XML for transformation using Categorizer's XSLT style sheets. The transformation is necessary because the Export XML schemas, Flexiondoc and SearchML, are not in a form easily searched by Content Categorizer rules.

For a list of file formats supported by OutsideIn XML Export, see Input File Formats.

8.2.7.2 Transformation Using XSLT Style Sheets

Two style sheets are included with Content Categorizer and applied based on the initial translation format provided by the OutsideIn XML Export filter. The style sheets are located in the following directory:

`/IntradocDir/data/contentcategorizer/stylesheets/`

For content items output in SearchML, *searchml_to_scc.xsl* is applied. For content items output in Flexiondoc, *flexiondoc_to_scc.xsl* is applied. SearchML and Flexiondoc both reproduce style designations found in the source content, but they do so differently, in ways not detectable by Content Categorizer rules. The appropriate style sheet can recognize the necessary style information in each format and use that information as the basis for transforming the final output tags into an XML document useful to Content Categorizer.

The similarity between SearchML and Flexiondoc depends on the degree to which internal styles or metadata are used in the content. When working with content using named styles, such as Microsoft Word, the resultant output is similar. When working with content in formats such a PDF or text, results come out with more generic tagging.

> **Important:**
>
> There is a problem with the XSLT transformation used to post-process PDF content that is output in Flexiondoc format. When Flexiondoc is used, single words are assigned to individual XML elements, making the final XML unsuitable for most Categorizer search rules. It is recommended to use SearchML for categorizing PDF content.

8.2.7.3 SearchML Transformation

When the OutsideIn XML Export filter translates content into SearchML XML format, it identifies the properties of the content item, such as title, subject, and author, and tags them as a <doc_property> element. It distinguishes the properties by a `type` attribute. It also identifies document text and tags it as a <p> element. It distinguishes styles within text by an `s` attribute.

8.2.7.4 Flexiondoc Transformation

When the OutsideIn XML Export filter translates content into Flexiondoc XML format, it identifies the properties of the content item, such as title, subject, and author, and tags them as a <doc_property> element, just like SearchML. However, it distinguishes the properties by a `name` attribute, instead of `type`.

Where Flexiondoc differs from SearchML is in how it identifies styles. Paragraph styles are tagged with <tx.p> tags, and character styles are tagged with <tx.r> tags, but each have an attribute based on a unique style `id`, in addition to a `name` attribute.

All styles are defined in child elements of the <style_tables> element of the Flexiondoc XML file, and given an `id` attribute, which is called when referencing the style, and which the template file uses to define a style key with a `name` attribute.

8.3 Using the Link Manager Component

Link Manager is an optional component bundled with and automatically installed with Content Server. When the component is enabled, it evaluates, filters, and parses the URL links of indexed content items before extracting them for storage in a database table (ManagedLinks). After the ManagedLinks table is populated with the extracted URL links, the Link Manager component references this table to generate link search results, lists of link references for the Content Information page, and the resource information for the Link Info page.

The Link Manager component enables users to:

- View lists of links using specific search criteria
- View detailed information about a specific link
- Recompute and refresh links to reevaluate and validate them
- View the links to other content in a specific content item
- View the links back to a specific content item

The search results, link references lists, and Link Info pages are useful to determine what content items are affected by content additions, changes, or revision deletions. For example, before deleting a content item, you can verify that any URL references contained in it are insignificant. Another use might be to monitor how content items are being used.

The Link Manager component extracts the URL links during the indexing cycle, so only the URL links of released content items are extracted. For content items with multiple revisions, only the most current released revision has entries in the database table. If the Link Manager component is installed after content items are checked in, perform a rebuild to ensure that all links are included in the ManagedLinks table.

Link Manager does all of its work during the indexing cycle and it increases the amount of time required to index content items and to rebuild collections.

The amount of time required depends on the type and size of the content items involved. That is, if the file is converted, this requires more time than text-based (HTML) files.

For information about disabling Link Manager during the rebuild cycle, see the `LkDisableOnRebuild` and`LkReExtractOnRebuild` variables.

This section discusses the following topics:

- Link Extraction Process
- Configuring Link Manager
- Link Administration

8.3.1 Link Extraction Process

> **Caution:**
>
> The Link Manager component uses HtmlExport 8 for file conversion. A link extractor template file is included with the Link Manager component. HtmlExport 8 requires this template. Do not edit this file.

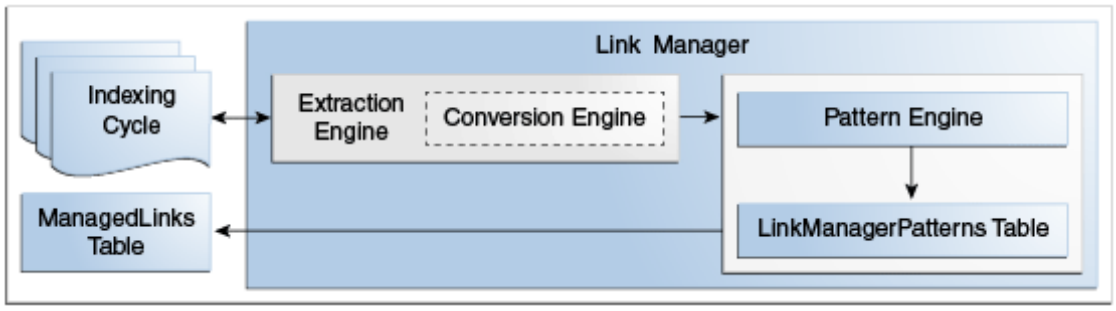
The Link Manager consists of an extraction engine and a pattern engine. The extraction engine includes a conversion engine (HtmlExport). The conversion engine is used to convert files that the extraction engine cannot natively parse to a text-based file format (HTML).

Link Manager does not use HtmlExport to convert files that contain any of the following strings in the file format: `hcs`, `htm`, `image`, `text`, `xml`, `jsp`, and `asp`. These text-based files are handled by Link Manager without need for conversion.

During the indexing cycle, the Link Manager component searches the checked-in content items to find URL Links as follows:

1. The extraction engine converts the file using the conversion engine (if necessary).
2. The extraction engine then uses the pattern engine to access the link evaluation rules defined in the Link Manager Patterns table.
3. The evaluation rules tell the extraction engine how to sort, filter, evaluate, and parse the accepted URL links in the content items.
4. The accepted URL links are inserted or updated in the ManagedLinks table.

Figure 8-1 The Link Manager Process



> **Note:**
>
> To execute successfully, HtmlExport requires either a virtual or physical video interface adapter (VIA). Most Windows environments have graphics capabilities that provide HtmlExport access to a frame buffer. UNIX systems, however, may not have graphics cards and do not have a running X-Windows Server for use by HtmlExport. For systems without graphics cards, you can install and use a virtual frame buffer (VFB).

8.3.1.1 File Formats and Conversion

Various file formats (such as Word) must be converted by the conversion engine (HtmlExport) before links can be extracted. Because Link Manager can extract links in text-based files (HTML) without requiring conversion, Link Manager does not use HtmlExport to convert files that contain any of the following strings in the file format: `hcs`, `htm`, `image`, `text`, `xml`, `jsp`, and `asp`.

Link Manager also handles all the variations of these file formats. For example, the `hcs` string matches the dynamic server page strings of `hcst`, `hcsp`, and `hcsf`. The image string matches all comparable variants such as `image/gif`, `image/jpeg`, `image/rgb`, `image/tiff`, and so on. To prevent other types of files from being converted, use the `LkDisallowConversionFormats` configuration variable. For more information, see *Configuration Reference for Oracle WebCenter Content*.

Link Manager recognizes links in the following file formats:

- Text-based formats (`txt`, `html`, `xml`, `jsp`, `asp`, `csv`, `hcst`, `hcsf`, and `hcsp`)
- Email (`msg` and `eml`)
- Microsoft Word
- Microsoft Excel

8.3.1.2 Link Status

All new and existing links are managed during the indexing cycle. When content items are checked in, the accepted links in the content items are added to or updated in the Managed Links table. Existing links are evaluated for changes resulting from content items being checked in or deleted. As links are added or monitored, they are marked as valid or invalid.

When one content item in the system references another content item in the system, the resulting link is marked as valid. When an existing link references a deleted content item, the link is reevaluated and the status changes from valid to invalid. Statuses are recorded as Y (valid) or N (invalid) in the `dLkState` column of the Managed Links table and displayed for the user in the `State` column of the Link Info page as `Valid` or `Invalid`.

8.3.2 Configuring Link Manager

You can specify the following Link Manager configuration variables in the *`IntradocDir`*`/config/config.cfg` file:

- `AllowForceDelete`
- `HasSiteStudio`

- `LkRefreshBatchSize`
- `LkRefreshErrorsAllowed`
- `LkRefreshErrorPercent`
- `LkRefreshErrorTHreshold`
- `LkDisableOnRebuild`
- `LkDisallowConversonFormats`
- `LkReExtractOnRebuild`
- `LkIsSecureSearch`

For information about using these configuration variables, see *Configuration Reference for Oracle WebCenter Content*.

8.3.2.1 Link Patterns

The Link Manager component uses an extraction engine that references the link patterns defined in a resource table. These link patterns are rules that tell the extraction engine how to sort the different links, which links to filter out, which links to accept, and how to parse the links for more information.

To customize the *`DomainHome`*`/ucm/LinkManager/resources/linkmanager_resource.htm` resource table, you can add new rules or edit the existing default rules. Customize the table using standard component architecture. The table includes the following columns.

Column Name	Description
lkpName	The name of the pattern and the primary key of the table. Used mainly in error handling and to allow other components to directly target the override of a specified rule.
lkpDescription	An explanation of the purpose of the pattern.
lkpType	The initial screening of the URL: • Prefix: If the path begins with a specified parameter, the condition is met. • Contains: If the path contains a specified parameter, then the condition is met. • Service: If the URL contains a value for IdcService and if this value matches a parameter, the condition is met. The extraction engine is a two-step engine. The 'prefix' and 'contains' types are used on the path part of the URL, while the 'service' type is used on the query string part of the URL.

Column Name	Description
lkpParameters	A comma-delimited list of patterns or parameters used by the type. The parameters are Idoc Script capable and are initially evaluated for Idoc Script. The engine uses the following rules for extracting the patterns from the parameters: • The parameter string is evaluated for Idoc Script. • The parameters are parsed using the comma separator. The result is a list of patterns. • Each pattern is XML decoded. One rule looks for a URL that begins with the resolved value for <$HttpRelativeWebRoot$> by setting `lpkParameters` to <$HttpRelativeWebRoot$>. A later rule can look for a URL that literally begins with <$HttpRelativeWebRoot$> by setting the parameter to `<$HttpRelativeWebRoot$>`
lkpAccept	Determines if the URL is accepted if the pattern is matched: • Pass: No determination is made. The 'action' is used to determine how this URL is processed. • Filter: the URL is rejected. This value is usually combined with `lkpContinue=false` to stop the processing. • Accept: The URL is accepted.
lkpContinue	Determines if the pattern processing engine continues to parse the URL. If true, the processing continues. If false, processing stops.
lkpLinkType	Specifies the URL type determined for this link.
lkpAction	A function defined in the LinkHandler class referring to a method in the LinkImplementor class used to further parse and evaluate the URL. LinkImplementor can be class aliased or extended.
lkpOrder	The order in which the patterns are to be evaluated.
lkpEnabled	Determines if this rule is evaluated. It is calculated and evaluated during start up when the patterns are loaded.

You can add new rules or edit the existing default rules using standard component architecture.

8.3.2.2 Database Tables

Two database tables are maintained with Link Manager:

- **Managed Links Table**: A link is stored in the Managed Links table if the pattern engine successfully processes it and determines that the link is acceptable. Each link in the table is assigned a unique class id (dLkClassId) and each row in the table has a unique GUID (dLkGUID). A single link can consist of multiple rows in the table if multiple resources define the link and each resource can independently break the link.

  For example, in Site Studio, you can define a single link by both a node and a content item. If the node is missing, the link breaks. If the content item is missing, the link breaks. In this case, there are two resources that do not depend on each other and each can break the link. Consequently, each resource is managed separately in the ManagedLinks table.

To improve query execution performance, standard indexes are added to the dDocName and dLkResource columns in the Managed Links table. System administrators are responsible for adjusting these indexes to accommodate specific database tuning requirements in various system environments.

- **Link Reference Count Table**: This table maps the content items to the number of times each is referenced in the ManagedLinks table. A content item in this table might not be a content item that is currently managed by Content Server. If there is an entry for a content item in this table, it only indicates that a link in the ManagedLinks table, as parsed by the pattern engine, has referenced the content item as a 'doc' resource.

  When a content item is checked in and a link references it, the link is marked as valid. When a link references a deleted content item, the link is marked as invalid. Notice that the dLkState column indicates the link's status as Y (valid) or N (invalid).

8.3.2.3 Link Manager Filters

The Link Manager component provides filters for parts of the pattern engine that allow customization of some very specific behavior. In general, the rules of the pattern engine are usually the ones to be modified. In certain circumstances Link Manager explicitly creates and uses filters to augment its standard behavior.

- extractLinks Filter: Used during the extraction process when the extraction engine parses the accepted URL links. As links are extracted, Link Manager looks for specific HTML tags. However, other HTML tags might also contain relevant links. If so, use this filter to extract the additional links.

  The tag is passed to the filter as a cached object with the key `HtmlTag`. The value (or link) is passed back to the parse with the key `HtmlValue`. If the filter extracts extra information, be aware that the passed-in binder is flushed before being passed to the pattern engine. The `service.setCachedObject` and `service.getCachedOject` methods should pass and retrieve the extra information, respectively.

  By default, it looks for the following HTML tags: <a>, <link>, <iframe>, <img>, <script>, and <frame>.

- linkParseService Filter: Used during the extraction process when the pattern engine evaluates links that use the `IdcService` parameter. After evaluation, the link binder and service are provided for the `linkParseService` filter.

  The service contains the binder for the parsed URL and information map. Customize the values in the parsed URL binder by adjusting certain parameters or customize the information map (which tells the parseService method what parameters to extract from the URL binder and how to map the data to resource types).

- sortAndDecodeLinks filter: Only available from the 'refresh' option. It is only called when users are refreshing the links. The service contains the 'LinkSetMap' which includes a sorted list of links contained in the ManagedLinks table. The refresh validates the Site Studio links and the existence of all links referring to 'doc' resources. You can create a component that augments the standard validation.

8.3.3 Site Studio Integration

> **Important:**
>
> When using Site Studio, set the `HasSiteStudio` configuration variable value to *true*. This variable enables the Site Studio-specific patterns for parsing 'friendly' URLs for the pattern engine. For more information about the `HasSiteStudio` variable, see *Configuration Reference for Oracle WebCenter Content*.

When configured to work with Site Studio, Link Manager obtains links from Site Studio by directly requesting a parsing of the links that Site Studio has identified. In return, Site Studio provides information about the links pertaining to its operation and components. In particular, Site Studio provides information about the node/section, if a content item is used, the state of the content item, the type of link (friendly, page, or node), and if the link is valid.

Site Studio does not load its project information when the Standalone applications are launched. Therefore the Site Studio links are not properly evaluated if a rebuild or index update cycle is started and completed by a standalone application.

When a user changes links using the Site Studio designer, Link Manager checks filter events. If a node is deleted, Link Manager marks all links using the deleted node as invalid, thus managing links that directly reference the node ID. Additionally, with information provided by Site Studio, Link Manager can accurately determine the state of the link.

Friendly URLs (links that do not reference the node ID or dDocName) are more difficult to manage and validate. When a node property changes, Link Manager marks all friendly links (both relative and absolute) that use the node as invalid and broken. Link Manager cannot retrace the parent chain to determine what part of the link was changed, how to fix it, or determine if it is actually broken.

Site Studio uses two types of managed links:

- Completely Managed Links: These are any links using the SS_GET_PAGE IdcService or links to nodes that include the following:
  - javascript:nodelink(Node,Site)
  - javascript:nodelink(Node)
  - ssNODELINK/Site/Node
  - ssNODELINK/Node

  Also links to pages that include the following:
  - ssLINK/Doc
  - ssLINK/Node/Doc
  - ssLINK/Site/Node/Doc
  - ssLink(Doc)
  - ssLink(Doc,Node)
  - ssLink(Doc,Node,Site)
  - javascript:link(Doc)

  - javascript:link(Doc,Node,Site)
- Provisionally Managed Links: The following Site Studio links are managed up to Site Studio node changes. Use the 'refresh' option from the Managed Links Administration page to determine state of the links. If the majority of links are of this form and nodes have changed dramatically, you should refresh or recompute the links.
  - Absolute (or full URLs): http://site/node/doc.htm
  - Friendly links to nodes

    <!--$ssServerRelativeSiteRoot-->dir/dir/index.htm

    [!--$ssServerRelativeSiteRoot--]dir/dir/index.htm

    <%=ssServerRelativeSiteRoot%>dir/dir/index.htm
  - Friendly links to pages

    <!--$ssServerRelativeSiteRoot-->dir/dir/doc.htm

    [!--$ssServerRelativeSiteRoot--]dir/dir/doc.htm

    <%=ssServerRelativeSiteRoot%>dir/dir/doc.htm

8.3.4 Link Administration

This section covers the following topics:

- Alternative Refresh Methods
- Recomputing and Refreshing Links in the ManagedLinks Table

8.3.4.1 Alternative Refresh Methods

In addition to the refresh activities available on the Managed Links Administration page, you can use alternative methods to update the Managed Links and Link Reference Count tables:

- Using the Repository Manager, perform a collection rebuild. This process rebuilds the entire search index, and the old index collection is replaced with a new index collection when the rebuild successfully completes.

  If Repository Manager is opened as a standalone application, the alternate refresh method can only be used when the `HasSiteStudio` configuration variable is disabled. When information is requested from Site Studio and the Repository Manager is in standalone mode, Site Studio is not initialized completely and does not return accurate information. This issue does not occur if the Repository Manager applet is used.
- If custom fields have been added while content is in the system, use the Configuration Manager **Rebuild Search Index** to rebuild the search index.

8.3.4.2 Recomputing and Refreshing Links in the ManagedLinks Table

To reevaluate the links in the ManagedLinks table:

1. Use the main menu to choose **Administration** then **Managed Links Administration**.
2. On the Managed Links Administration page, use an option to manage links:

- **To recompute links**: Click **Go** next to the **Recompute links** option. This refresh activity resubmits each link in the ManagedLinks table to the patterns engine. The link is evaluated according to the pattern rules and updated in the table. A link can be reclassified as another type of link depending on which patterns have been enabled or disabled. Use this option if the pattern rules have changed.
- **To refresh links**: Click **Go** next to the **Refresh links** option. This activity checks each link in the ManagedLinks table and attempts to determine if the link is valid. For Site Studio links, the links are sent to the Site Studio decode method to determine what nodes and content items are used by the link. It also determines if the link is valid and is indeed a Site Studio link.

  Use this option after many changes to Site Studio node/section properties. LinkManager cannot completely track the changes to 'friendly' Site Studio links. By refreshing or forcing a validation on the links, Link Manager can more accurately determine which links are broken and which are valid.
- **To refresh the references counts**: Click **Go** next to the **Refresh** option. This activity flushes the LinkReferenceCount table and queries the ManagedLinks table for the content item references. Both the 'recompute' and 'refresh' table activities try to maintain the LinkReferenceCount table. However, on occasion, this table can become out-of-sync and this option, when used on a quiet system, rebuilds this table.gv
- **To cancel a refresh activity**: Click **Go** next to the **Abort activity** option. Only one refresh activity can be active at any one time.

The Status area indicates how many links have been processed and how many errors have been encountered.

Only one refresh activity can be active at any one time. Wait until the refresh activity completes and the `Ready` status is displayed before attempting another refresh activity.

9
Tracking Content Access

This chapter describes how to obtain information about the activity of content items in a Content Server instance, which can be tracked using the Oracle WebCenter Content Server Content Tracker component.
This chapter covers the following topics:

- About Content Tracker
- Understanding the Content Tracker Functionality
- Operational Details
- Data Tracking Functions

9.1 About Content Tracker

Content Tracker is an optional component automatically installed with Oracle WebCenter Content Server. The Content Tracker component when enabled provides information about system usage such as which content items are most frequently accessed and what content is most valuable to users or specific groups. Knowing the consumption patterns of an organization's content enables more effective delivery of appropriate, user-centric information.

For detailed information about customizing Content Tracker, see *Developing with Oracle WebCenter Content*.

9.2 Understanding the Content Tracker Functionality

Content Tracker monitors activity on a Content Server instance and records selected details of those activities. It then generates reports that illustrate the way the system is being used. This section includes an overview about Content Tracker and Content Tracker Reports functionality.

Content Tracker incorporates several optimization functions which are controlled by configuration variables. The default values for the variables set Content Tracker to function as efficiently as possible for use in high volume production environments. For more information about Content Tracker configuration variables, see *Configuration Reference for Oracle WebCenter Content*.

This section covers the following topics:

- Content Tracker
- Data Recording and Reduction
- Content Tracker Terminology
- Installation Considerations

9.2.1 Content Tracker

Content Tracker monitors a system and records information collected from different sources about activities. The information is merged and written to a set of tables in the Content Server database. Content Tracker can monitor activity based on:

- **Content item usage:** Data is obtained from Web filter log files, the Content Server database, and other external applications such as portals and websites. Content item access data includes dates, times, content IDs, and current metadata.
- **Services:** Services that return content, and services that handle search requests, are tracked. By default, Content Tracker logs only the services that have content access event types but by changing the configuration, Content Tracker can monitor any service, even custom services.
- **User accesses:** Information is gathered about non-content access events, such as the collection and synthesis of user profile summaries. This data includes user names and user profile information.

9.2.2 Data Recording and Reduction

Content Tracker *records data* from the following sources:

- **Web server filter plug-in:** When content is requested with a static URL, the Web server filter plug-in records request details, saving the information in event log files. The event log files are used as input by the Content Tracker data reduction process.
- **Service handler filter:** Content Tracker monitors services that return content. When one of these services is called, details of the service are copied and saved in the SctAccessLog table.
- **Logging service:** Content Tracker supports a single-service call to log an event. You can call it directly with a URL, as an action in a service script, or from Idoc Script.
- **Database tables:** When configured to collect and process user profile information, a data reduction process queries selected database tables to obtain information about active users during the reporting period.
- **Application API:** An interface is available to register other components and applications for tracking. This interface allows cooperating applications, such as Site Studio, to log event information in real time. The application API is designed as a code-to-code call which does not involve a service. The API is not meant for general use. If you are building an application and are interested in using this interface, contact Consulting Services.

The *data reduction process* gathers and merges the data obtained from the data recording sources. Until this reduction process has finished, the data in the Content Tracker tables is incomplete. The reduction is run one time for each day's data gathered. You can run the reduction manually, or schedule it to run automatically, usually during an off-peak period when the system load is light.

9.2.3 Content Tracker Terminology

The following terminology is used with Content Tracker:

- **Data collection:** Gathering content access information and writing the information to event log files.
- **Data reduction:** Processing the information from data collection and merging it into a database table.
- **Data Engine Control Center:** The interface that provides access to the user-controlled functions of the Data Engine. It has the following tabs:
  - **Collection:** Used to enable data collection.
  - **Reduction:** Used to stop and start data reduction (merging data into database tables).
  - **Schedule:** Used to enable automatic data reduction.
  - **Snapshot:** Used to enable activity metrics. The term snapshot also denotes an information set representing the world at a particular time.
  - **Services:** Used to add, configure, and edit service calls to be logged. It is also used to define the specific event details logged for a given service.
- **Service definitions:** The ResultSet structure in the service call configuration file (`SctServiceFilter.hda`) that contains entries to define each service call to be logged. The service definition ResultSet is named ServiceExtraInfo.
- **Service entry:** The entry in the service definition ResultSet (ServiceExtraInfo) that defines a service call to be logged. The ServiceExtraInfo ResultSet contains one service entry for each service to be logged.
- **Field map:** A secondary ResultSet in the service call configuration file (`SctServiceFilter.hda`) that defines the service call data and the specific location where data is to be logged.
- **Top Content Items:** Most frequently accessed content items in the system.
- **Content Dashboard:** A page that provides overview information about the access of a specific content item.

9.2.4 Installation Considerations

Content Tracker is supported on most hardware and networked configurations but some hardware and software combinations require special consideration:

- Tracking Limitations in Single-Box Clusters
- Static URLs and WebDAV
- ExtranetLook Component
- Search Relevance Metrics

Set the `SctUseGMT` configuration variable to true to use Greenwich Mean Time (GMT). It is set to false by default, to use local time. For more information about configuration variables see *Configuration Reference for Oracle WebCenter Content*.

When upgrading from an earlier version of Content Tracker there is a one-time retreat (or advance, depending on location) in access times. To accommodate the biannual daylight savings time changes, discontinuities in recorded user access times are used (contingent on the use of local time and the location).

9.3 Operational Details

Depending on Content Tracker configuration, it can perform Data Collection of event information such as dynamic and static content accesses and service calls. Both types of data are recorded in a Combined Output Table(SctAccessLog). Service calls are inserted into the log in real time but the static URL information must first undergo the Data Reduction process (either manual or scheduled).

After activity data is collected, Content Tracker combines, analyzes and synthesizes the event information and loads the summarized activity into database tables.

- Data Collection
- Data Reduction
- Content Tracker Event Logs
- Combined Output Table
- Data Output
- Tracking Limitations

9.3.1 Data Collection

Data collection is the initial step in any tracking function. Content Tracker data collection includes collecting information from static URL references and service call events. Data is collected using several different methods:

- Service Handler Filter
- Web Server Filter Plug-in
- Logging Service

9.3.1.1 Service Handler Filter

Using the service handler filter, Content Tracker obtains information about dynamic content requests that come through the Web server, and also about other types of activity, such as calls from applications. The service request details are obtained from the DataBinder that accompanies the service call, and the information is stored in the Combined Output Table (SctAccessLog) in real time.

The `SctServiceFilter.hda` configuration file is used to determine which service calls are logged. It uses a ResultSet structure that includes one service definition entry for each service to be logged. When using the extended service logging function, the file also contains field maps corresponding to service definition entries.

The ServiceExtraInfo ResultSet is included in the `SctServiceFilter.hda` file. This ResultSet contains one or more service entries defining the services to be logged. Additional field map ResultSets are used to support the extended service logging function. Each service that has additional data values tracked must have a field map ResultSet in the `SctServiceFilter.hda` file to define the data fields, locations, and database destination columns for the related service.

9.3.1.2 Web Server Filter Plug-in

Managed content retrieved with a static URL does not usually invoke a service. The Content Tracker Web server filter plug-in collects the access event details (static URL references) and records them in raw Content Tracker Event Logs (sctlog files). The information in these files requires an explicit reduction (either interactive or scheduled) before it is included in the Combined Output Table with the service call data.

9.3.1.3 Logging Service

The logging service is a single-service call that can be called directly with a URL or as an action in a service script. It can also be called from Idoc Script using the `executeService` function. The calling application is responsible for setting the fields to be recorded in the service DataBinder, including the descriptive fields listed in the Content Tracker service filter configuration file (`SctServiceFilter.hda`).

There should be no duplication or conflicts between services logged with the service handler filter and those logged with the Content Tracker logging service. If a service is named in the Content Tracker service handler filter file then such services are automatically logged so there is no need for the Content Tracker logging service to do it. However, Content Tracker does not attempt to prevent such duplication.

9.3.1.4 Enabling or Disabling Data Collection

To enable or disable data collection:

1. Choose **Administration** then **Content Tracker Administration** from the Main menu. Choose **Data Engine Control Center**.
2. On the Data Engine Control Center: **Collection** tab, select (to enable collection) or clear (to disable collection) the **Enable Data Collection** check box.
3. Click **OK**.

   Do not exit the applet. Wait until a confirmation message displays. If you exit before the confirmation message, the requested change(s) may not occur.
4. After the confirmation message is displayed, click **OK**.
5. Restart the Web server and Content Server, in that order.

9.3.2 Data Reduction

During data reduction, the static URL information captured by the Web server filter plug-in is merged and written into the output table the service call data. Depending on configuration, at the time of the reduction the Content Tracker user metadata database tables are also updated with information collected from the static URL accesses and from the service call event records:

- Standard Data Reduction Process
- Data Reduction Process with Activity Metrics
- Data Reduction Cycles
- Access Modes and Data Reduction
- Reduction Sequence for Event Logs

- Reduction Schedules
- Running Data Reduction Manually
- Setting Data Reduction to Run Automatically
- Deleting Data Files

9.3.2.1 Standard Data Reduction Process

During the data reduction process, the static URL information is extracted from the raw data files and combined with the service information stored in the SctAccessLog table. By default, Content Tracker collects and records data only for the SctAccessLog table. Although the user data output tables exist, Content Tracker does not populate them.

Depending on how Content Tracker is configured, this reduction process can:

- Combine access information for static URL content access with service details.
- Summarize information about user accounts that were active during the reporting period. This information is written to the Content Tracker's user metadata database tables.

9.3.2.2 Data Reduction Process with Activity Metrics

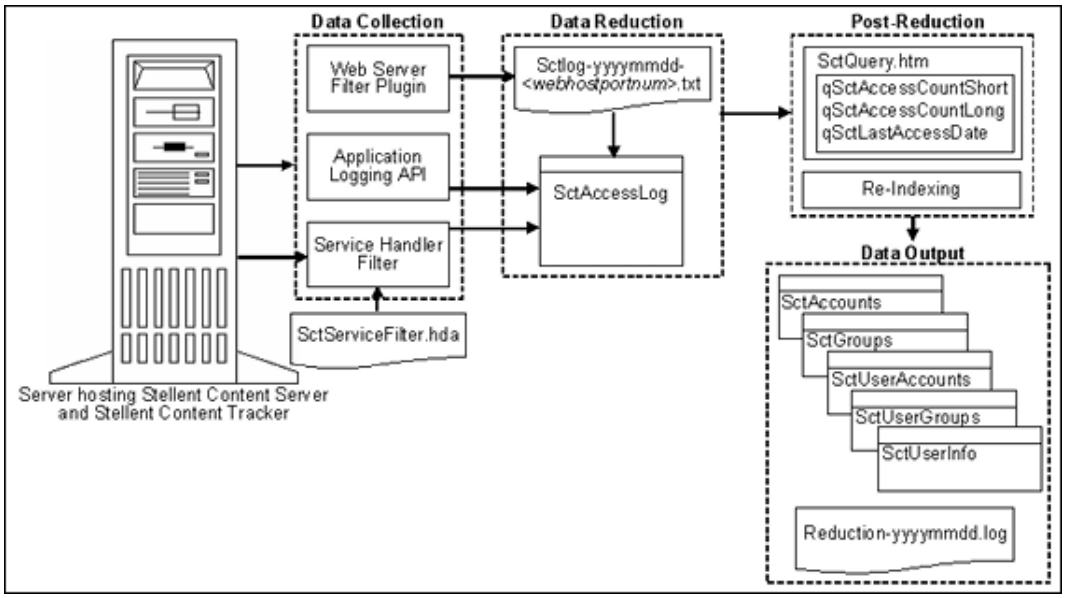
Content Tracker provides the option to selectively generate search relevancy data and store it in custom metadata fields. You can use the snapshot function to choose which activity metrics to activate. The logged data provides content item usage information that indicates the popularity of content items.

By default, Content Tracker collects and records data only for the SctAccessLog table. Although the user data output tables exist, Content Tracker does not populate them unless the Snapshot function is activated. However, using the snapshot function affects Content Tracker's performance.

If the snapshot function and activity metrics are activated, the values in the custom metadata fields are updated following the reduction processing phase. When users access content items, the values of the applicable search relevance metadata fields change. During the later post-reduction step, Content Tracker uses SQL queries to determine which content items were accessed during the reporting period. Content Tracker updates the database table metadata fields with the new values and initiates a re-indexing cycle. However, only the content items whose access count metadata values have changed are re-indexed.

The post-reduction step is necessary to process and tabulate the activity metrics for each affected content item and to load the data into the assigned custom metadata fields. It also initiates a re-indexing cycle on the content items with changed activity metrics values to ensure that the data is part of the search index and is accessible to select and order search results.

Figure 9-1 Data Reduction Process with Activity Metrics



9.3.2.3 Data Reduction Cycles

Reduced table data is moved from the primary tables to the corresponding archive tables when the associated raw data is moved from recent to archive status. The primary tables contain the output for reduction data in the new and recent cycles and the archive tables contain output for reduction data in the archive cycle.

Raw data is demoted from new to recent when the data is reduced and it is older than day. Thus, the 'new cycle' indicates that the data is for the current day or is unreduced data from previous dates. The 'recent cycle' indicates that the data is from yesterday or earlier and has been reduced.

Raw data is demoted to archive (and the corresponding rows in the SctAccessLog table are moved to the SctAccessLogArchive table) when the number of recent sets reaches a configured threshold number and a reduction process is run, either manually or through the scheduler. For more information about configuring the threshold number for recent sets, see the `SctMaxRecentCount` configuration variable information in *Configuration Reference for Oracle WebCenter Content*. If a reduction process is never run, the raw data remains in the recent cycle indefinitely.

9.3.2.4 Access Modes and Data Reduction

The access mode used to access content items determines how those accesses are recorded in the SctAccessLog table. If content items are accessed through a service (that is, viewing the actual native file), the events are recorded in the SctAccessLog table in real time. In this case, the activity is recorded immediately and is not dependent on the reduction process.

If content items are accessed using static URLs (that is, viewing the Web location file), the Web server filter plug-in records the events in a static log file. During the data reduction process, the static log files for a specified date are gathered and the data is moved into the SctAccessLog table. In this case, if data reduction is not performed for a given date, there are

no static URL records in the SctAccessLog and no evidence that these accesses ever occurred.

The difference in the way static and service accesses are processed has implications for interval counts. For example, a user might access a content item twice on Saturday, one time through the Web location file (static access) and one time through the native file (service access). The service access is recorded in the SctAccessLog table but the Web location access is not. If Sunday's data is reduced, only the service access (not the static access) is included in the summaries of the short and long access count intervals. However, if Saturday's data is also reduced, both the service and static accesses are recorded in the SctAccessLog table and included in the both intervals.

9.3.2.5 Reduction Sequence for Event Logs

Data sets are usually reduced in chronological (calendar) order to ensure that the information included in reports is current. The order in which the raw data log files are reduced determines what specific user access data is logged and counted. During reduction, the SctAccessLog and user metadata database tables are modified with data from the raw data files.

When using the snapshot function to gather search relevance information, the metadata fields associated with the activated activity metrics are also updated during data reduction. The activity metrics use custom metadata fields included in the DocMeta database table.

Content Tracker changes the activity metrics values according to the applicable data in the reduction data set. To ensure that data values are complete and current, perform data reduction on a daily basis. If the data sets are reduced out of order, re-reducing the current or most recent data set corrects the counts. However, it is always preferable to consistently reduce data in calendar order.

The following scenarios show how the reduction sequence affects the stored data.

Scenario 1:

Depending on how content items are accessed, if activity on certain days (such as Saturdays and Sundays) is never reduced, then accesses that occur on those days might never be logged or counted. For more information, see Access Modes and Data Reduction. Similarly, if a content item is accessed on Tuesday and reductions are done for Monday and Wednesday, the Tuesday access is might not be counted toward the last access of that content item.

Scenario 2:

If there was a significant increase in accesses in the last few days, and you reduce data from two weeks earlier, the long and short access metrics for content items do not reflect the recent activity. Instead, the interval values from two weeks earlier override today's values. Reducing the current or most recent data set corrects the counts.

The reduction order does not adversely affect the Last Access date. The reduction process only changes the Last Access date if the most recent access in the reduction data set is more recent than the current Last Access value in Content Server's DocMeta database table.

If you have reduced a recent data set and a particular content item had been accessed, the Last Access field is updated with the most recent access date in the

reduction data set. If you then re-reduce an older data set, the older access date for this content item does not overwrite the current value.

Scenario 3:

Reducing the data sets in an arbitrary order interferes with the demotion of "recent" data files to "archive" data files. The movement of the associated table records is based on the age, archive tables are intended to store the "oldest" data. If the data sets are reduced in random order, it is not apparent which data is the oldest.

For more information about recent and archive data files, see User Metadata Tables and Data Reduction Cycles.

9.3.2.6 Reduction Schedules

You can configure reduction runs to run on a scheduled basis to periodically reduce the raw data. A steady flow of raw data goes into the recent and archive repositories, and a similarly steady flow of reduced data goes from the primary tables to the archive tables.

Note that if the Content Tracker Data Engine is disabled the day before a scheduled reduction run, no data is collected. If it is enabled on the day of the scheduled reduction run, the scheduler does not run because no data is available.

Data reductions scheduled for a given day are performed on data collected during the previous day. The previous day is defined as the 24-hour period beginning and ending at midnight (system time). To conserve CPU resources, you can schedule reduction runs for early morning hours when the system load is generally the lowest.

An error can be issued if the scheduled reduction is set to run within a few minutes after midnight. If this occurs, reschedule the reduction to run later.

9.3.2.7 Running Data Reduction Manually

To manually reduce data:

1. Choose **Administration** then **Content Tracker Administration** from the main menu. Choose **Data Engine Control Center**.
2. On the Data Engine Control Center: **Reduction** tab, click (to highlight) the set of input data to reduce. Information on this page includes the following:
   - **Cycle**: The status of the input data. Values include *new* (the input data has not been reduced), *recent* (data has been reduced but is not archived), and *archive* (data has been reduced and remains in archive cycle until deleted).
   - **Available date**: Date when the data was collected.
   - **Status**: The status of the reduction. Values include *ready* (input data is available to be reduced), *running* (data is being reduced), and *archiving* (data is being moved from *recent* to *archive* cycle).
   - **Percent Done**: the progress of the reduction cycle.
   - **Completion Date**: Date and time the reduction completed.
3. Click **Reduce Data**.
4. Click **Yes** to reduce the data.

> **Note:**
>
> If the current date's data is reduced, the status in the Cycle column stays as 'new' even though the data is reduced.

9.3.2.8 Setting Data Reduction to Run Automatically

To set data reduction to run automatically:

1. Choose **Administration** then **Content Tracker Administration** from the main menu. Choose **Data Engine Control Center**.
2. On the Data Engine Control Center: **Schedule** tab, select the S**cheduling Enabled** check box.
3. Select check boxes for the days when data reduction occurs.
4. Select the hour and minute when data reduction occurs.
5. Click **OK**.

   Do not exit the applet. Wait until a confirmation message displays. If you exit before the confirmation message, the requested change(s) may not occur.
6. Click **OK** when the confirmation message is displayed.

9.3.2.9 Deleting Data Files

To delete data files:

1. Choose **Administration** then **Content Tracker Administration** from the main menu. Choose **Data Engine Control Center**.
2. On the Data Engine Control Center: **Reduction** tab, click (to highlight) the set of input data to delete.
3. Click **Delete** or **Delete Archive**.
4. Click **OK** to delete the data.

9.3.3 Content Tracker Event Logs

Content Tracker supports multiple input files for different event log types and for configurations with multiple Web servers. Each Web server filter plug-in instance uses a unique tag as a file name suffix for the event logs. The unique suffix contains the Web server host name plus the server port number.

The reduction process searches for and merges multiple raw event logs named `sctLog-yyyymmdd-`*`myhostmyport`*`.txt`. The raw event logs are processed individually.

Content Tracker may not always capture a user name for a content access event, even if the user is logged into Content Server. In this case, the item was accessed with a static URL request and, in general, the browser does not provide a user name unless the Web server asks it to send the user's credentials. If the item is public content, the Web server does not ask the browser to send user credentials, and the user accessing the URL is unknown.

To record the user name for every document access, make sure the content is not accessible to the guest role. If the content is not public, the user's credentials are required to access the items and a user name is recorded in the raw event log entry.

Depending on Content Tracker configuration, when raw data log files in the new cycle are reduced, the Data Engine moves the data files into the following subdirectories:

- The default number of data sets that the `recent/` directory can hold is 60 sets (dates) of input data log files. When the number of data sets is exceeded, the eldest are moved to the `/archive` directory.

  cs_root`/data/contenttracker/data/recent/`*yyyymmdd*`/`

- By default, Content Tracker does not archive data. Instead, the expired rows are discarded to ensure optimal performance. If appropriately configured, Content Tracker uses the `archive/` directory to hold all input data log files that were moved out of the "recent" cycle.

  cs_root`/data/contenttracker/data/archive/`*yyyymmdd*`/`

When raw data files are reduced, another file (*reduction_ts-yyyymmdd.txt)* is generated as a time stamp file.

9.3.4 Combined Output Table

The SctAccessLog table contains entries for all static and dynamic content access event records. The SctAccessLog table is organized using one line per event in the reporting period. The rows in the table are tagged according to type:

- S indicates the records logged for service calls.
- W identifies the records logged for static URL requests.

By default, Content Tracker does not log accesses to GIF, JPG, JS, CSS, CAB, and CLASS file types. Therefore, entries for these file types are not included in the combined output table after data reduction.

The Content Tracker Web server filter plug-in cannot distinguish between URLs for user content and those used by the user interface. References to UI objects, such as client.cab, can appear in the static access logs. To eliminate these false positives, use the `SctIgnoreDirectories` configuration variable to define a list of directory roots to be ignored by the Content Tracker filter. To log these file types, change the default setting for the `SctIgnoreFileTypes` configuration variable to the type (gif,jpg,js,css). For more information about using configuration variables, see *Configuration Reference for Oracle WebCenter Content*.

The following table describes the information collected for each record in the SctAccessLog table. By default, Content Tracker does not collect data to populate certain columns for bulky and rarely used items.

Column Name	Type /Size	Column Definition
SctDateStamp	datetime	Local date when data collected in format YYYYMMDD, depending on customer location and time of day event occurs. This may differ from date recorded for eventDate. Time set to 00:00:00 Data source: Internal
SctSequence	int /8	Sequence unique to entry type Data source: Internal

Column Name	Type /Size	Column Definition
SctEntryType	char /1	Entry type. Values are W or S Data source: Internal
eventDate	datetime	GMT time and date when request completed. The date depends on customer location and time of day event occurs. This may differ from date recorded for SctDateStamp)
SctParentSequence	integer	Sequence of outermost Service Event in tree, if any.
c_ip	varchar /15	IP of client
cs_username	varchar /255	
cs_method	varchar /10	GET
cs_uriStem	varchar /255	Stem of URI
cs_uriQuery	varchar / [maxUrlLen]	Query portion. For example, `IdcService=GET_FILE&dID=42...`
cs_host	varchar /255	Content Server server name
cs_userAgent	varchar /255	Client User Agent Ident By default, this column contains either `browser` or the suffix of any string beginning with `java:`. This simplification ensures optimal performance for Content Tracker.
cs_cookie	varchar / [maxUrlLen]	Current cookie
cs_referer	varchar / [maxUrlLen]	URL leading to this request
sc_scs_dID	int /8	dID Data source: from query or derived from URL (reverse lookup)
sc_scs_dUser	varchar /50	dUser Data source: Service DataBinder `dUser`
sc_scs_idcService	varchar /255	Name of IdcService. For example, `GET_FILE` Data source: from query or Service DataBinder `IdcService`
sc_scs_dDocName	varchar /30	dDocName Data source: from query of Service DataBinder `dDocName`
sc_scs_callingProduct	varchar /255	Arbitrary identifier Data source: SctServiceFilter config file or Service DataBinder `sctCallingProduct`
sc_scs_eventType	varchar /255	Arbitrary identifier Data source: SctServiceFilter config file or Service DataBinder `sctEventType`
sc_scs_status	varchar /10	Service execution status Data source: Service DataBinder `StatusCode`
sc_scs_reference	varchar /255	`web`, `native`, `sdc_url` Values indicate the rendition of the accessed file. `web` is a converted file (PDF), `native` is the original file and `sdc_url` is HTML. Data source: algorithmically from query parameters or ServiceFilter config file

Column Name	Type /Size	Column Definition
comp_username	varchar /50	Computed user name. If a Service, obtained from UserData Service Object or HTTP_INTERNETUSER or REMOTE_USER or dUser. If a static URL, obtained from auth-user or internetuser.
comp_validRef	char /1	Indicates if the referenced object exists and is available to the requesting user. 1 if the access was a Web reference (W), and ispromptlogin and isaccessdenied are both NULL, and the static URL exists at reduction time. Or, if the access was a service call (S) and the sc_scs_status field is NULL. NULL if the static URL did not exist at reduction time, or the user logon failed, or the logon succeeded but the user was not authorized to view the object.
sc_scs_isPrompt	char /1	1 if true Data source: Plug-in immediateResponseEvent field "ispromptlogin"
sc_scs_isAccessDenied	char /1	1 if true Data source: Plug-in immediateResponseEvent field isaccessdenied
sc_scs_inetUser	varchar /50	Internet user name (if security problem) Data source: Plug-in immediateResponseEvent field internetuser
sc_scs_authUser	varchar /50	Authorization user name (if security problem) Data source: Plug-in immediateResponseEvent field auth-user
sc_scs_inetPassword	varchar /8	Internet password (if security problem) Data source: Plug-in immediateResponseEvent field internetpassword
sc_scs_serviceMsg	varchar /255	Content Server service completion status Data source: Service DataBinder StatusMessage
extField_1 through extField_10	varchar /255	General purpose columns to use with the extended service tracking function. In the field map ResultSets, the DataBinder fields are mapped to these columns.

9.3.5 Data Output

When Content Tracker is appropriately configured, the static and dynamic content access request information and all metadata fields are accessible. The logged metadata includes content item and user metadata:

- Content Item Metadata
- User Metadata Tables
- Reduction Log Files

9.3.5.1 Content Item Metadata

Content Tracker uses standard Content Server metadata tables for content item metadata.

9.3.5.2 User Metadata Tables

Content Tracker user metadata database tables are updated with information collected about active users during the reporting time period. These tables retain data about user profiles at the time the data reduction runs. The names of the user metadata tables are formed from a

root which indicates the class of information contained, and an `Sct` prefix to distinguish the table from native Content Server tables.

By default, Content Tracker does not archive data so expired rows are not moved from the Primary tables to the Archive tables. Instead, the expired rows are discarded, ensuring optimal performance. Two complete sets of user metadata database tables are created:

- **Primary**: Named SctUserInfo, and so on, which contain the output for reduction data in the new and recent cycles.
- **Archive**: Named SctUserInfoArchive, and so on, which contain output for reduction data in the archive cycle.

If Content Tracker is configured to run archives, reduction data files are moved from *recent* to *archive* status and the associated table records are moved from the Primary table to the Archive table. This prevents excessive buildup of rows in the Primary tables, and ensures that queries performed against recent data complete quickly. Rows in the Archive table are not deleted. They can be moved or deleted using any SQL query tool. To delete all the rows in the Archive tables, delete the tables themselves. They are re-created during the next Content Server restart. Reports are not run against archive data.

The following tables are created:

- The SctAccounts table contains a list of all accounts. It is organized using one line for each account.
- The SctGroups table contains a list of all user groups current at time of reduction. It is organized using one line per content item group.
- The SctUserAccounts table contains entries for all users listed in the SctUserInfo table and who are assigned accounts defined in the current instance. A separate entry exists for each user-account combination.

  In multiple proxy instances, the group and account information of a user may not be determined by Content Tracker. When the current instance is a proxy, the group information for an active user defined in a different proxy is replaced by a placeholder line in SctUserGroups for that user. The line contains the user name and a hyphen (-) placeholder for the group. If at least one account is defined in the current instance, a similar entry is created in SctUserAccounts for any user who is defined in a different proxy.
- The SctUserGroups table is organized using one line for each user's group for each user active during the reporting period. It references those users who logged on during the data collection period. If Content Tracker is running in a proxied Content Server configuration, only groups defined in the current instance are listed. For example, a user named "joe" is defined in the master instance and has access to groups "Public" and "Plastics" in the master instance. If "joe" logs on to a proxy instance and the group "Plastics" is not defined in the proxy, only the association between "joe" and "Public" appear in SctUserGroups.
- The SctUserInfo table is organized using one line per user. It includes all users known to the current instance and additional users from a different instance who logged on to the current instance during the data collection period. In a proxied configuration, users local to one instance are usually visible from the UserAdmin application to other instances. If a user is defined locally with the same name in two instances, only the local user is visible in each of these instances.

For example, the "sysadmin" defined in the master is not the "sysadmin" appearing in the UserAdmin application for a proxy. These two different users could both log in during the same data collection period. The user from the master logs on as "sysadmin" and the proxy user logs on as "cs_2/sysadmin" (for example). The `SctUserInfo` file generated for this period has separate entries for "sysadmin" and "cs_2/sysadmin".

9.3.5.3 Reduction Log Files

When data reduction is run, the Content Tracker Data Engine generates a summary results log file, named *`reduction-yyyymmdd`*`.log`. The reduction logs can be useful to help diagnose data reduction errors.

9.3.6 Tracking Limitations

In some cases, Content Tracker has limitation in tracking data. This section provides an overview of those limitations.

- Tracking Limitations in Single-Box Clusters
- Static URLs and WebDAV
- Data Directory Protections
- ExtranetLook Component

9.3.6.1 Tracking Limitations in Single-Box Clusters

Currently, Content Tracker does not support multi-node clusters that are installed in a single server. This is true even though multiple network cards are installed and each cluster node has its own IP address. In this case, the Content Server instance for each cluster node can successfully bind its IntradocServerPort to its specific IP address.

Unfortunately, only one cluster node is able to bind its Incoming Provider ServerPort to its specified IP address. Consequently, all of the cluster nodes share and alternately use the same Incoming Provider ServerPort. As a result, the SctLock provider for Content Tracker can only track document accesses on one cluster node at a time.

9.3.6.2 Static URLs and WebDAV

The access counts determined by Content Tracker are generally correct, but in some circumstances the software cannot determine if the content was actually delivered to the requesting user, or if it was, which revision of the content was delivered:

- Repeated requests through WebDAV: If a user accesses a document with a WebDAV client then re-accesses the same document later, only the first WebDAV request is recorded. Access count reports for such content are usually lower than the actual number.
- Static URLs: A user saves a URL for a content file, but the content is later revised in such a way that the saved URL is no longer valid. If the user attempts to access the content with the saved URL, an error occurs. Content Tracker records this as a successful access even though content was not delivered. Access count reports for such content are usually higher than the actual number.
- Static URLs and wrong dID: If a user accesses content using a URL and the content is revised or the security group is changes before the Content Tracker data reduction operation is performed, the user is reported as seeing the latest revision. Access count

reports for such content are usually attributed to a newer revision than actual. To minimize this effect, schedule or run data reductions on a regular basis.

This section covers the following topics:

- Wrong dID Reported for Access by Saved Static URL
- False Positive for Access by Saved (stale) Static URL
- Missed Accesses for Content Repeatedly Requested via WebDAV

9.3.6.2.1 Wrong dID Reported for Access by Saved Static URL

Scenario: User accesses content via the "Web Location" (URL). The content is then revised before the Content Tracker data reduction operation is performed. The user is reported as seeing the latest revision, not the revision that the user actually saw. Access counts reported for such content tend to be attributed to a newer revision than actual. Minimize this effect by scheduling or running Content Tracker data reductions on a regular basis.

Details: This is related to False Positive for Access by Saved (stale) Static URL, described above. That is, the web server uses the entire web location, (for example, *DomainHome*`/ucm/cs/groups/public/documents/adacct/`*xyzzy*`.doc`), to locate and deliver the content, while Content Tracker uses only the ContentID portion to determine the dID and dDocName values. Moreover, Content Tracker makes this determination during data reduction, not at the time the access actually occurs.

There are some implications of this not immediately obvious, such as when the group and/or security of the revision are changed from the original. For example, if a user accesses "Public" Revision 1 of a document through a static URL, and the document is subsequently revised to Revision 2 and changed to "Secure" before the Content Tracker data reduction takes place, Tracker reports that the user saw the Secure version. This may also occur when the content file type changes. If the user accesses an original `.xml` version, which is then superseded by an entirely different `.doc` before the data reduction is performed, Tracker reports the user saw the `.doc` revision, not the actual `.xml` version.

9.3.6.2.2 False Positive for Access by Saved (stale) Static URL

Scenario: User saves a "Web Location" (URL) for a content file. The content is subsequently revised in such a way that the saved URL is no longer valid. The user then attempts to access the content through the (now stale) URL, and gets a "Page Cannot be Found" error (HTTP 404). Content Tracker may record this as a successful access even though the content was not actually delivered to the user. Access counts reported for such content tend to be higher than actual.

Details: The "Web Location" of a content file is the means by which a user can access content via a "static URL". The specific file path in the URL is used in two, slightly different contexts: It is used by the web server to locate the content file in the Content Server repository, and it is also used by Content Tracker to determine the dID and dDocName of the content file during the data reduction process. The problem occurs when the content is revised in such a way that the web location for a given Content ID changes between the time the URL is saved and the time the access is attempted.

For example, if a Word document is checked in then revised to an XML equivalent, the web location for the latest revision of the content changes from the first line of code shown to the second line of code shown, where "xyzzy" is the assigned Content ID.

DomainHome/ucm/cs/groups/public/documents/adacct/*xyzzy*.doc

DomainHome/ucm/cs/groups/public/documents/adacct/*xyzzy*.xml

The original revision is renamed as:

DomainHome/ucm/cs/groups/public/documents/adacct/*xyzzy*~1.doc

This means the original Web Location no longer works as a static URL. The Content ID obtained from the original URL, however, matches the latest revision.

9.3.6.2.3 Missed Accesses for Content Repeatedly Requested via WebDAV

Scenario: User accesses a document via a WebDAV client, then accesses the same document in the same manner later. Only the first WebDAV request for the document is recorded. Access counts reported for such content tend to be lower than actual.

Details: WebDAV clients typically use some form of object 'caching' to reduce the amount of network traffic. If a user requests a particular object, the client first determines if it already has a copy of the object in a local store. If it does not, the client contacts the server and negotiate a transfer. This transfer is recorded as a COLLECTION_GET_FILE service request.

If the client already has a copy of the object, it contacts the server to determine if the object has changed since the client local copy was obtained. If it has changed, then a new copy is transferred and the COLLECTION_GET_FILE service details is recorded.

If the client copy of the object is still current, then no transfer takes place, and the client presents the saved copy of the object to the user. In this case, the content access is not counted even though the user appears to get a "new" copy of the original content.

9.3.6.3 Data Directory Protections

Content Tracker's Web server filter plug-in runs in the authorization context of the user whose access request is being processed. In some cases, the owner of the request processing thread is a system account. In others, it is a requesting user or another type of non-system account used by the application.

The filter records the information in raw event logs. If the log file does not exist a new one is created using the default protection and authorization credentials of the user who owns the event thread. If the user account has write permission to the data directory, the content access data is recorded. Otherwise, the logging request fails and the access event details are not recorded.

To ensure that Content Tracker can properly record user access requests, the data directory must be configured to accept the account authorization credentials for all users. Granting world write permission (or the equivalent) is one method. Allowing unlimited write access is recommended unless security concerns prohibit this level of unrestricted access.

9.3.6.4 ExtranetLook Component

The ExtranetLook component (if enabled) allows customizations of cookie-based login forms and pages for anonymous-type users. The component uses a built-in Web server plug-in that monitors requests and determines if a request is authenticated based on cookie settings. When a user requests access to a content item, Content Tracker must function within the authorization context of the user's account.

After collecting the access information, Content Tracker tries to record the event data in the log file. If the user's account permissions allow access to Content Tracker's data directory, then the request activity is logged. However, if the account does not have write authorization, the logging request fails and the request activity is not recorded.

9.4 Data Tracking Functions

This section describes the different data tracking functions available with Content Tracker:

- Activity Snapshots
- Service Calls
- Web Beacon Functionality

9.4.1 Activity Snapshots

The activity snapshots feature captures user metadata that is relevant for each recorded content item access:

- Search Relevance Metrics
- Enabling the Snapshot Function
- Creating the Search Relevance Metadata Fields
- Setting a Check-in Time Value for the Last Access Field
- Populating the Last Access Field for Batch Loads and Archives
- Linking Activity Metrics to Metadata Fields
- Editing the Snapshot Configuration

9.4.1.1 Search Relevance Metrics

When activated, the activity metrics and corresponding metadata fields provide search relevance information about user accesses of content items. An optional automatic load function allows users to update the last access activity metric to ensure that checked-in content items are appropriately time-stamped.

Content Tracker optionally fills the search relevance custom metadata fields with content item usage information that indicates the popularity of particular content items. This information includes the date of the most recent access and the number of accesses in two distinct time intervals.

Information generated from these activity metrics functions is used in various ways. For example, you can order search results according to which content items have been recently viewed or the most viewed in the last week.

If the snapshot function is activated, the values in the search relevance metadata fields are updated during a post-reduction step. During this processing step, Content Tracker uses SQL queries to determine which content items have changed activity metrics values. Content Tracker updates the applicable database tables with the new values and initiates a re-indexing cycle. However, only the content items that have changed metadata values are re-indexed.

9.4.1.2 Enabling the Snapshot Function

To use these optional features, first enable the snapshot post-processing function which activates the activity metrics choices. Then selectively enable the activity metrics and assign their preselected custom metadata fields.

To enable the snapshot function and activate the activity metrics:

1. Choose **Administration** then **Content Tracker Administration** from the main menu. Choose **Data Engine Control Center**.
2. On the Data Engine Control Center: **Snapshot** tab, select **Enable Snapshot**.
3. Click **OK**.
4. In the confirmation window, click **OK**.

9.4.1.3 Creating the Search Relevance Metadata Fields

Before implementing the snapshot function, decide which custom metadata fields to associate with each of the enabled activity metrics. Also, the custom metadata fields must exist and must be of the correct type. Depending on which activity metrics to be enabled, create one or more custom metadata fields using an applicable procedure.

Add the following specific information for the activity metrics:

- Last Access Metric
  - Field Type: Date
  - Default Value: Optional. If not specified, the field is not populated until a content item is checked in and a data reduction run. Some applications require a default value and in those cases, enter a value in the Default Value field that ensures the Last Access field is populated with the date and time of the content check in. For more information, see Setting a Check-in Time Value for the Last Access Field.
  - Enable for Search Interface: Optional. Check to make the field available for searching.
- Short and Long Access Metric
  - Field Type: Integer
  - Enable for Search Interface: Optional. Check to make the field available for searching.

Indexing a custom metadata field is optional, although indexing makes searches on this field more efficient. Indexing also allows users to query the accumulated search relevance statistics and generate useful data. For example, you can create a list of content items ordered by their popularity, and so on.

9.4.1.4 Setting a Check-in Time Value for the Last Access Field

The Last Access Date field is normally updated by Content Tracker when a managed object is requested by a user and a data reduction run. The field can be empty (NULL) until the next data reduction is run. Some applications require that the date and time of content check in be recorded immediately in the Last Access field.

Use any of the following methods to populate the Last Access field:

- Using the Configuration Manager: When adding the metadata field, enter an expression that populates the field with the date and time of content check in (for example, a default value of `<$dateCurrent()$>` populates the field with the current check-in date and time). After setting the value, fill the field for existing content using the Autoload option.
- Using the Autoload option: This option allows retroactive replacement of NULL values in the Last Access field with the current date and time. The only records affected are those where the Last Access metadata field is empty (NULL)

  1. Choose **Administration** then **Content Tracker Administration** from the Main menu. Choose **Data Engine Control Center**.
  2. Click the Data Engine Control Center: **Snapshot** tab.
  3. Select one or more of the activity metric check boxes to enable them. Enter the name of the custom metadata field to be linked to the activity metric (for example, `xLastAccess`, `xShortAccess`, or `xLongAccess`).
  4. Select the **Autoload** check box.
  5. Click **OK**.

     A confirmation dialog box opens and the current date and time are inserted into the applicable Last Access fields (those with NULL values) in the DocMeta database table.

     Please note:

     - Autoload is primarily intended for use with applications that count check-in operations as an access activity.
     - Autoload backfills the current date and time for all existing content that does not have a date value in the Last Access field. Any content checked in after the Last Access field is defined should have the field automatically populated with the check-in date and time as a default value.
     - Running Autoload can affect every record in the DocMeta database table. Use this option sparingly.
     - The only DocMeta records affected are those where the Last Access metadata field is empty (NULL).
     - Autoload is persistent. The state of the Autoload check box is saved with all the other Snapshot settings. To prevent inadvertent use of this option, clear the Autoload check box and re-save activity metrics field settings immediately after performing the autoload function.
     - Content Server's indexer is not automatically run after Autoload completes the update. You must decide when to rebuild the collection.
     - By default, the Autoload query sets the Last Access metadata field to the current date and time. You can customize the query as needed.

9.4.1.5 Populating the Last Access Field for Batch Loads and Archives

To ensure proper retention of archived and batch loaded content, set the Last Access field date for the import/insert. Otherwise the access date for these content items is NULL, and retention based on this field fails. Also consider how the date can affect retention management. For example, an import of 1998 data is probably better tagged with that date than the date when the import was performed to accurately reflect the retention quality of the content.

The name of the Last Access field is based on the name specified when the field was created. For example, if the name Last Access is used, xLastAccess would be used in the import/insert.

For more information about using the Batch Loader utility, see *Administering Oracle WebCenter Content*.

The following steps provide a general outline of the procedure to populate the Last Access field using Batch Loader:

1. Access the Batch Loader.
2. Create a record that establishes an appropriate Last Access date. For example:

```
# This is a comment
Action=insert
dDocName=Sample1
dDocType=ADACCT
xLastAccess=5/1/1998
dDocTitle=Batch Load record insert example
dDocAuthor=sysadmin
dSecurityGroup=Public
primaryFile=links.doc
dInDate=8/15/2001
<<EOD>>
```

3. Run the Batch Loader to process the file record.

9.4.1.6 Linking Activity Metrics to Metadata Fields

After the activity metrics options have been activated, they must be individually selected to enable them. Enabling the activity metrics also activates their corresponding custom metadata fields.

To enable the activity metrics and activate their corresponding custom metadata fields:

1. Choose **Administration** then **Content Tracker Administration** from the main menu. Choose **Data Engine Control Center**.
2. Click the Data Engine Control Center: **Snapshot** tab.
3. Select one or more of the activity metric check boxes to enable them. Enter the name of the custom metadata field to be linked to the activity metric (for example, `xLastAccess`, `xShortAccess`, or `xLongAccess`).
4. For the Short and Long Access Counts, enter the applicable interval amounts in days. For example, 7 days for the Short Access Count and 28 days for the Long Access Count.

   The two Access Count metrics differ only in the accounting period (for example, last 30 days versus last 90 days, last week versus last year, and so on). The time intervals specified in the activity metrics are independent of each other. For example, you can set the number of days in the first interval period (Short Access) to more than those in the second interval period (Long Access).

   Access counts are only tabulated for reduced dates. If data is not reduced for one or more days, the accesses on those days are not logged or counted. Do not reduce data in random order because the Access Count metrics are affected by the reduction date order.
5. Click **OK** when done.
6. In the confirmation window, click **OK**.

Note that the fields are case-sensitive. Make sure all field values are spelled and capitalized correctly.

Content Tracker uses the following error checks to validate each enabled activity metric field value:

- Checks the DocMeta database table to ensure that the custom metadata field actually exists.
- Ensures that the custom metadata field is of the correct type (for example, that the Last Access metadata field is of type Date, an so on).
- Checks to explicitly exclude the dID metadata field.

9.4.1.7 Editing the Snapshot Configuration

To modify the snapshot activity metrics settings:

1. Choose **Administration** then **Content Tracker Administration** from the main menu. Choose **Data Engine Control Center**.
2. Click the Data Engine Control Center: **Snapshot** tab.
3. Make the necessary changes in the activity metrics fields.
4. Click **OK**.
5. In the confirmation window, click **OK**.

9.4.2 Service Calls

Content Tracker enables the logging of service calls with data values relevant to the associated services. Every service to be logged must have a service entry in the service call configuration file (SctServiceFilter.hda). In addition to the logged services, you can include the corresponding field map ResultSets in the SctServiceFilter.hda.

For more information about managing service calls, see *Developing with Oracle WebCenter Content*.

9.4.3 Web Beacon Functionality

> **Important:**
>
> The implementation requirements for the Web beacon feature are contingent on the system configurations involved. All of the factors cannot be addressed in this documentation. Information about the access records collected and processed by Content Tracker are an indication of general user activity and not exact counts.

A Web beacon is a managed object that facilitates specialized tracking support for indirect user accesses to Web pages or other managed content. In earlier releases, Content Tracker was unable to gather data from cached pages and pages generated from cached services. When users access cached Web pages and content items, Content Server and Content Tracker are unaware that these requests ever happened.

Without using Web beacon referencing, Content Tracker does not record and count such requests.

The Web beacon involves the use of client side embedded references that are invisible references to the managed beacon objects within Content Server. Content Tracker can record and count user access requests for managed content items that have been copied by an external entity for redistribution without obtaining content directly from Content Server.

Web beacon functionality is useful for reverse proxy activity.

Two situations in particular merit the use of the Web beacon functionality: reverse proxy activity and when using Site Studio.

In a reverse proxy scenario, the reverse proxy server is positioned between the users and Content Server. The reverse proxy server caches managed content items by making a copy of requested objects. The next time another user asks for the document, it displays its copy from the private cache. If the reverse proxy server does not have the object in its cache, it requests a copy.

Because it is delivering cached content, the reverse proxy server does not directly interact with Content Server. Therefore, Content Tracker cannot detect these requests and does not track this type of user access activity.

A reverse proxy server is often used to improve Web performance by caching or by providing controlled Web access to applications and sites behind a firewall. Such a configuration provides load balancing by moving copies of frequently accessed content to a Web server where it is updated on a scheduled basis.

For the Web beacon feature to work, each user access includes an additional request to the managed beacon object in Content Server. The additional request adds overhead, but the Web beacon object is very small and does not significantly interfere with the reverse proxy server's performance. Note that it is only necessary to embed the Web beacon references in objects you specifically want to track.

If your Website is intended for an external audience, you may decide to create a copy of the site and transfer it to another server. In addition to being viewed publicly, this solution also ensures that site development remains separate from the production site. In this arrangement, however, implement the Web beacon feature to ensure that Content Tracker can collect and process user activity.

For more information about managing Web beacon objects, see *Developing with Oracle WebCenter Content*.

10
Managing Content Profiles

This chapter explains how to use content profiles to selectively include or reorder metadata fields to produce targeted Check In, Update, Content Information, and Search pages in Oracle WebCenter Content Server.
This chapter covers the following topics:

10.1 About Content Profiles

Administrators can use content profiles to selectively include or reorder metadata fields to produce targeted Check In, Update, Content Information, and Search pages. Content profiles do not create or modify any Oracle WebCenter Content Server tables. They are simply used as a type of filter for what information is displayed. All information for a content profile is stored in the *IntradocDir*`/data/profiles/document/` directory.

After you create a content profile, it is always active. You can disable the link on the user interface, but the profile rules remain functional unless the profile is deleted.

10.2 Content Profile Elements

A profile is composed of rules and a trigger value, which are set up on the **Profiles** and **Rules** tabs of the Configuration Manager page. Administrators can create multiple content profiles and all are available to the end user. For each profile, the end user has a distinct check-in page and search page available. Although all profiles are visible to all users, each user can configure their user interface to hide or display links to specified profiles.

> **Note:**
>
> Documents cannot be associated with multiple profiles in the system.

Content profiles are composed of the following:

- **Rules**: A rule consists of a set of metadata fields that determine if fields are editable, required, hidden, excluded, or read-only based on their criteria when specific conditions

are met. You can change a rule's behavior based on an input, or *activation condition*. You can evaluate a rule for every profile (*global*), or you can evaluate the rule for specific profiles. For ease of use, you can use rules to group metadata fields under an optional header.

For example, a profile's rules can determine the user type and, depending on the document type being checked in, ensure that only specific metadata fields are displayed. Rules must be established before a profile is created.

- **Triggers**: A *trigger field* is a metadata field that is defined on the Configuration Manager: Profiles tab. If a document matches a *trigger value* for a profile, then that profile is evaluated for the document. There can be an unlimited number of profiles, but only one trigger value per profile.

  Although you create rules before you create triggers and profiles, it is necessary to know what your trigger is before creating rules.

10.2.1 Using a Profile Link

When a profile is enabled on the Edit Content Profile Links page, the profile is available from the Search and New Check In menus on the toolbar. If no profiles are enabled for display, the Search and New Check In menus become direct links to the Advanced Search page and standard Content Check In Form, respectively.

After a profile has been created, it appears in the Search and New Check In menus on the toolbar after refreshing the browser session. By default, all profiles are listed as options under both menus. However, not every user is authorized to use all of the listed profiles. On the Edit Content Profile Links page, select or clear applicable check boxes to specify the profiles to display.

For example, a marketing employee does not have the necessary privileges to use an accounting profile. In this case, the user can clear the check boxes for the accounting profile and it does not display under Search and New Check In menus. For more information about the user interface in general and the content profile links in particular, see *Using Oracle WebCenter Content*.

10.3 Content Profile Rules

> **Note:**
>
> Although you create rules before you create triggers and profiles, it is necessary to know what your trigger is before creating rules.

A profile consists of one or more rules and a trigger value. The rules determine how metadata fields are displayed on the Check In, Update, Content Information, and Search pages and if a rule is used (depending on how it is evaluated). Each rule consists of the following:

- A set of metadata fields. For more information, see Metadata Fields and Attributes in Rules.
- An optional activation condition. For more information, see Activation Conditions in Rules.

- An option that indicates if it is a global rule and has a specified priority.
- An option that indicates if the metadata fields in the rule are grouped and if an optional header is used.

Global rules are always 'on' (always evaluated). A global rule automatically affects the metadata fields displayed on the Check In, Update, Content Information, and Search pages even if it is not included in a profile or even if no profiles have been created. It is not necessary for a profile to exist in the system for any defined global rules to take effect and be applied to events, actions, or workflow states. However, you cannot preview the effects of a global rule unless it is associated with a profile.

Global rules are evaluated first and can be superseded by specific profile rules. The priority for the global rule can be set to increase its precedence. It can then have a higher priority than specific rules and produce different profile results. View those results by previewing the profile and seeing the consequence of rule selection.

A global rule obeys the following guidelines:

- It is always on, is independent of a profile, and is always evaluated.
- For documents and searches with profiles, the global rule is evaluated first. The specific profile rules are evaluated after the global rule. Global rules have a lower priority than profile rules.
- Global rules have a priority number. The priority determines the order in which the rule is evaluated. Lower priority rules are executed earlier and rules with higher priority can override changes made by rules with lower priority.

This section covers these topics about rules:

- Metadata Fields and Attributes in Rules
- Activation Conditions in Rules
- Restricted Lists in Rules
- Regular Expressions
- Using Rules to Group Metadata Fields

10.3.1 Metadata Fields and Attributes in Rules

Each metadata field in a rule has the following attributes:

- Field position (required): Adjusts the general placement order of the metadata field. Values are *top*, *middle*, and *bottom*.
- Display type (required): Determines how the metadata field is displayed on the Check In and Search pages.Values can be *Edit*, *Info Only*, *Hidden*, *Excluded*, or *Required*. If required, a message is also required.
- Use Default value (optional): Displays a default value for the metadata field.
- Is Derived value (optional): Enables the metadata field to be set to a specified value on update or check in.
- Has Restricted list (optional): Allows the list metadata field to be restricted to either a specific list of values or to a filtered list of values.

10.3.2 Activation Conditions in Rules

An activation condition allows a change in the profile behavior based on different inputs. For example, a rule is not active for the search page or for a contributor, or certain fields are hidden or overridden on check in. Also, because profiles are activated during any check-in process, distinctions are made between a browser check in and a batch-load check in.

You can preview profiles to assess the validity of the activation conditions. The previewing page is used to check the existing profile and perform what-if scenarios by changing activation condition choices and evaluating the results.

You can base an activation condition for a rule on:

- A system event: These include on-request events, on-submit events, and on-import events.
- A user action: These include check in new, check in selected, content information, content update, and search.
- A workflow state: These are contingent on if the content item is in a workflow.
- A document type: These can use components based on document metadata fields.
- A user type: These can use components based on user metadata fields.

> **Caution:**
>
> Be very careful when using activation conditions that include one or more combinations of condition choices. Not all combinations of activation condition choices are valid and some can be mutually exclusive. For example, if an activation condition requires the event to be an import and the action to be a document information page request, the activation is never true and the rule is never active.

10.3.3 Restricted Lists in Rules

The restricted list is an optional attribute for a metadata field in a rule. You can modify the user interface for metadata fields defined as lists in two ways:

- Specifying a fixed list: An explicit set of values that override the actual master list for the metadata field that was defined as a list. Only those items in the master list are displayed in the user interface list.
- Using regular expression evaluation: The list can include wildcards and other special characters for string pattern matching and evaluation processes. The items displayed in the user interface list are those values satisfying the regular expression.

10.3.4 Regular Expressions

Regular expressions are ideal for text manipulation and describe the format of strings. In its simplest form, a regular expression specifies the text to match.

For example, the regular expression 'ABC' matches the string ABC but not the string DEF. You can use wildcard characters, such as the asterisk (*), to match more strings. The asterisk (*) specifies zero or more instances of the preceding character or characters. For example, the regular expression 'A*B' matches the strings B, AB, AAB, AAAB, and so on.

This section provides a brief overview of using regular expression evaluation to generate modified user interface lists. Because of the complexity of regular expressions, system administrators must be familiar with regular expressions, building patterns, and implementing regular expression methods. If not, use Oracle Consulting Services to assist in defining restricted lists.

The following table lists the most commonly used modifiers, metacharacters, and special characters used in building patterns for regular expression evaluation.

Modifiers

Element	Definition
g	Global pattern matching.
i	Case-insensitive pattern matching.
m	Allows the special characters ^and $to match multiple times within a string.
s	Allows the special character . to match newlines.
x	Ignores whitespace within a pattern.

Metacharacters

Element	Definition
\s	Matches whitespace (including tabs and newlines).
\S	Matches anything that is not whitespace.
\b	Matches only a word boundary.
\B	Matches only nonword boundaries.
\d	Matches digits 0 through 9.
\D	Matches only nonnumeric characters.
\w	Matches only letters, numbers, or underscores.
\W	Matches only characters that are not letters, numbers, or underscores.
\A	Matches the beginning of a string only.
\Z	Matches the end of a string only.

Special Characters

Element	Definition
*	Matches zero or more occurrences of the preceding character.
+	Matches one or more occurrences of the preceding character.
?	Matches zero or one occurrence of any character.
.	Matches any one character, except newlines.
^	Matches the beginning of a string, like the \A metacharacter.
$	Matches the end of a string, like the \Z metacharacter.

Element	Definition
|	Imposes either, or.

The following examples illustrate the results displayed in the user interface lists depending on how the Edit Restricted List page is completed. The restricted lists being defined use a metadata field defined to be a list. Its master list values are the US states in alphabetical order. The two dependencies include:

- The items or expression entered into the text pane.
- The Allow Java Regular Expressions check box (selected or unselected).

Example 1

In this example, text values are entered into the text pane and the Allow Java Regular Expressions check box is not selected. In this case, the options 'NoState' and 'Carolina' are not included in the resulting list because they are not full names of states. Note that the order is maintained as typed into the text area.

If the following values are entered into the text pane:

- Alabama
- Minnesota
- NoState
- Utah
- Carolina

The results displayed in the user interface list are:

- Alabama
- Minnesota
- Utah

Example 2

In this example, the same text values are entered into the text pane as in Example 1. However, the Allow Java Regular Expressions check box is selected.

If the following values are entered into the text pane:

- Alabama
- Minnesota
- NoState
- Utah
- Carolina

The results displayed in the user interface list are:

- Alabama
- Minnesota
- Utah

- North Carolina
- South Carolina

In this case, both 'North Carolina' and 'South Carolina' are included in the resulting list because they match the regular expression 'Carolina'.

Example 3

In this example, the Allow Java Regular Expressions check box is selected and instead of entering similar text values (as in the previous examples) the ^special character is used with alphabet characters.

In this case, there are two regular expressions. The first expression specifies choosing everything in the master list beginning with C and the second expression specifies choosing everything beginning with Al. Notice that the results order is dictated by how the list was entered in the text pane.

If the following values are entered into the text pane:

- ^C
- ^Al

Then the results displayed in the user interface list are:

- California
- Colorado
- Connecticut
- Alabama
- Alaska

Example 4

In this example, the same values are entered into the text pane as in Example 3. However, both values are entered on the same line and separated with the pipe (|) special character which is evaluated as 'or'. In this case, the expression retains the values in order because the list is filtered exactly one time for values that begin with either Al or C.

If the following values are entered into the text pane:

- ^C |^Al

The following results are displayed in the user interface list:

- Alabama
- Alaska
- California
- Colorado
- Connecticut

10.3.5 Using Rules to Group Metadata Fields

You can group and arrange metadata fields and label them with an appropriate header. The fields are shown on the Check In, Update, Content Information, and Search pages as specified in the group.

To create metadata groups, select **Is Group** on the Edit Restricted List page. Use the **Fields** tab to add metadata fields to the group. Use the **Up** and **Down** buttons to rearrange the fields.

For example, Figure 10-1 shows a rule on the left that results in the metadata field list on the Check In page on the right. In this example, Content ID is the group leader because it is the first element in the group list. The metadata fields included after Content ID are the group associates.

Figure 10-1 Metadata Fields Generated from Rule

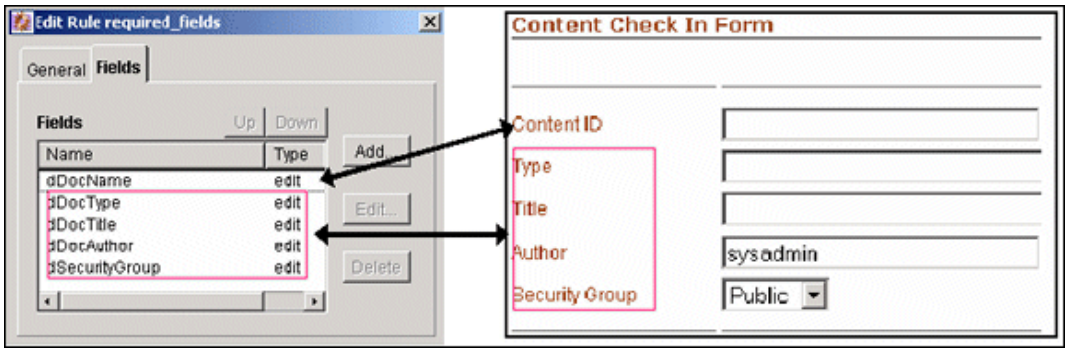
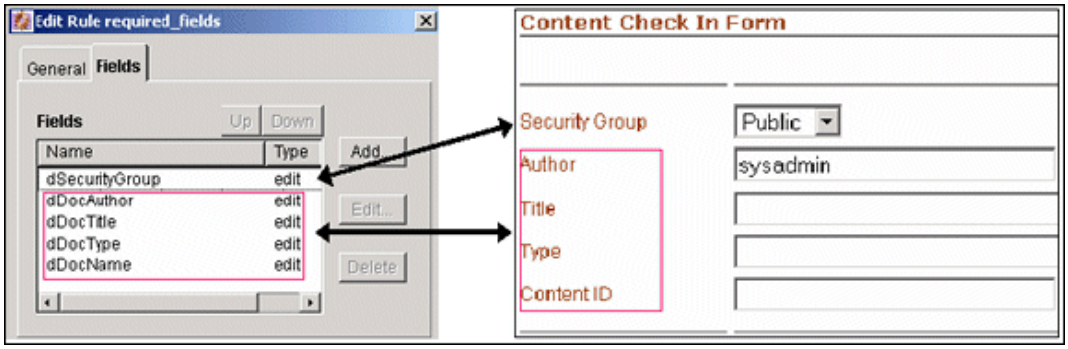


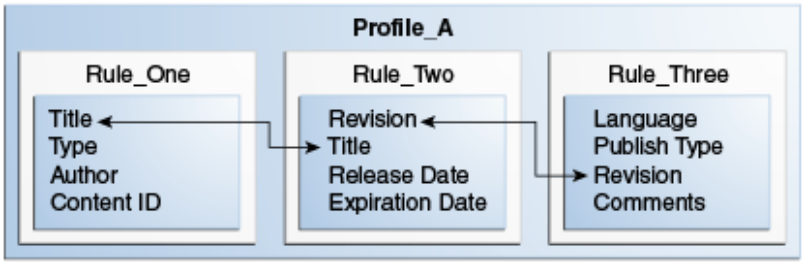
Figure 10-2 shows the same rule but the metadata fields in the group have been rearranged using the **Up** and **Down** buttons. This reorganization results in a different listing of the same metadata fields on the Check In page. In this case, Security Group becomes the group leader and the other fields are now the group associates.

Figure 10-2 Reorganized Metadata Fields



In Figure 10-3, a single profile contains three rules that have grouped metadata fields. Each group has one field that belongs to another group. In this situation, the system uses resolution rules to reconcile any conflicts.

Figure 10-3 Profile with Rules Grouping Metadata Fields



> **Caution:**
>
> System evaluation and implementation of additional profile and global rules that contain one or more of these metadata fields can cause grouping conflicts. Some rules executed later can override earlier rules and affect how grouped metadata fields are resolved.

The following rules resolve conflicts between metadata fields that belong to groups in multiple rules:

1. The first element in the list is the group leader.
2. All elements following the first element are the group associates.
3. If the group leader is not a group leader in another group listing, then assign any group associates to the group, below the group leader.
4. If a group leader is a group associate in a prior group listing, then the new group listing is merged with the prior group listing as follows:
   a. Find the main group leader (the group leader in the prior group).
   b. Insert the new group associates after the group leader in the main group leader's group associates list.
5. Ensure that no group associate has multiple group leaders. If so, remove the associate from the prior group leader's list.
6. If a grouping has a group associate that is a group leader in another later grouping, then this rule is invalid, an error is reported, and the rule is not evaluated. (If this were to be allowed, the result would be a non-group leader (a group associate) being promoted to a group leader.)

Example 1

1. **IF:** A,B,C is a metadata group

   WHERE: A is the group leader and B and C are group associates to A
2. **AND:** B,D,E is another metadata group

   WHERE: B is the group leader and D and E are group associates to B
3. **RESULT:** A,B,D,E,C

Example 2

1. **IF:** A,B,C is a metadata group

   WHERE: A is the group leader and B and C are group associates to A
2. **AND:** A,D,E is another metadata group

   WHERE: A is the group leader and D and E are group associates to A
3. **RESULT:** A,D,E,B,C

   Example 3

Example 3

1. **IF:** A,B,C is a metadata group

   WHERE: A is the group leader and B and C are group associates to A
2. **AND:** C,B,D is another metadata group

   WHERE: C is the group leader and B and D are group associates to C
3. **RESULT:** A,C,B,D

Example 4

1. **IF:** A,B is a metadata group

   WHERE: A is the group leader and B is a group associate to A
2. **AND:** B,A,C is another metadata group

   WHERE: B is the group leader and A and C are group associates to B
3. **RESULT:** Theoretically, this situation can resolve to B,A,C but this makes the A,B grouping irrelevant. To avoid confusion for other groupings, this is treated as an error case.

Example 5

1. **IF:** A,B,C is a metadata group

   WHERE: A is the group leader and B and C are group associates to A
2. **AND:** D,A,E is another metadata group

   WHERE: D is the group leader and A and E are group associates to D
3. **RESULT:** Error. It is impossible to resolve this grouping conflict.

10.4 Display Results of Reordered Metadata Fields

You can use content profiles to reorder metadata fields on the Check In, Update, Content Information, and Search pages. You can reorder custom metadata fields and system-specific information fields.

This section provides information about the display results of reordered custom and system information fields.

You can position metadata fields, as described in the following sections:

- General Sequence of Grouped Metadata Fields

10.4.1 General Sequence of Grouped Metadata Fields

The positioning of grouped system and custom metadata fields on Content Server pages is determined by the priority of the first metadata field in the group. When adding a custom metadata field to the system, its positioning sequence (field order) is set.

Add custom metadata fields using the Configuration Manager: I**nformation Field** tab and assign the sequence number in the Order field on the Add/Edit Metadata Field page.

When a custom metadata field is the first field in a group, that group is positioned on the page according to the field order assigned to the custom metadata field. When a system metadata field is the first field in a group, that group is positioned according to their established precedence.

Depending on the specific Content Server page, you can include or exclude specified system metadata fields in the general display order. For example, the Search page displays the Release Date and Expiration Date system metadata fields but excludes Revision.

By default, the general order for system metadata fields is as follows:

- Content ID (dDocName)
- Type (dDocType)
- Title (dDocTitle)
- Author (dDocAuthor)
- Security Group (dSecurityGroup)
- Account (dDocAccount)
- Revision (dRevLabel)

A group with a system metadata field as the first field is usually displayed in default order. For example, if *Author* is the first field in a group of custom metadata fields, that group is displayed below any group containing Content ID, Type, or Title as its first field.

10.4.2 Positioning Metadata Fields Within a Group

Using Rules to Group Metadata Fields describes how to define rules to conveniently group custom and system metadata fields on the Check In, Update, Content Information, and Search pages. You can also order metadata fields using the following methods:

- **Option 1: Field Position**: Use the Field Position list, available when adding metadata fields to rules using the Add Rule Field page. This option works in a relative manner. For example, you might add the following metadata fields:
  - xRegion (Top position)
  - xSubDept (Bottom position)

  If you add xDept with a field position of Middle, it is added as follows:
  - xRegion (Top position)
  - xDept (Middle position)

  - xSubDept (Bottom position)

  If you then add xContinent with a field position of Top, it is added as follows:

  - xRegion (Top position)
  - xContinent (Top position)
  - xDept (Middle position)
  - xSubDept (Bottom position)

  Similarly, if you add xManager with a field position of Middle, it is added as follows:

  - xRegion (Top position)
  - xContinent (Top position)
  - xDept (Middle position)
  - xManager (Middle position)
  - xSubDept (Bottom position)

  This option produces these display results on the Check In, Update, Content Information, and Search pages if the fields are grouped. When adding the fields to a rule, select **Is Group** on the Add/Edit Rule page.

- **Option 2: Up and Down buttons**: Use the **Up** and **Down** buttons to reorder fields. This option is available when adding metadata fields to rules using the **Fields** tab. It is often useful to reorder fields after they are added, or to reorder fields with the same field position.

  For example, if you added three fields with a field position of *Top*, they are positioned in the order they were added to the rule. However, you can use the **Up** button to move a field to the absolute top. Similarly, if any field is not positioned properly when it was added, you can use the **Up** and **Down** buttons to reposition them.

10.4.3 Display Results of Grouped Metadata Fields

The following rules specify how metadata groups are displayed on the Check in, Update, and Check in Selected pages.

- If the first field in a group is a system field (such as Content ID, Type, Title, and so on), the group is always displayed above the Primary File field.
- If automatic Content ID generation is disabled, then the Content ID field is always listed as the first field on the page followed by the remaining fields in the group. Also, if a separate group includes other system fields like Title and Type, that group is listed after the Content ID group but above the Primary File field.
- If automatic Content ID generation is enabled, then the Content ID field functions like a custom metadata field with 1 as its field order. In this case, if Content ID is the first field in a group, then the group is displayed immediately below the Primary File and Alternate File fields. Also, the Revision system metadata field is displayed after the last field in the Content ID group. (Note that, by default, Revision is displayed below the Alternate File field.)
- If the first field of a group is a custom metadata field, then the group is ordered by the field order number of the lead metadata field relative to the lead metadata fields in other groups, even if there are system metadata fields in the group.

- The Release Date and Expiration Date fields are always listed last on the page unless they are grouped with a custom metadata field that has a higher (that is, smaller number) field order value. Or, if Release Date and Expiration Date are grouped with a system metadata field, then they are listed above the Primary File field.

The following rules specify how metadata groups are displayed on the Search page.

- The Content ID field is always positioned first unless it is part of a group and it is not the first field. However, if Content ID is the first field of a group, then that group is listed first.
- If a system metadata field (other than Content ID) is the first field in a group, that group is listed after the Content ID field or Content ID group.
- All other groups with custom metadata fields as the first fields are displayed after groups with system metadata fields as the lead fields. When groups have a custom metadata field as the first field, the ordering of these groups is determined by the field order numbers of the lead metadata fields of groups in relation to each other.

In order for a metadata field to be displayed on a search page, the Enable for Search Index must be set on the Add/Edit Metadata Field page.

The following rules specify how metadata groups are displayed on the Content Information page.

- The Content ID field is always positioned first unless it is part of a group and it is not the first field.
- The Checked Out By, Status, and Formats fields are always listed at the bottom.
- The Security Group field, or any group with Security Group as the first field, is listed above the Checked Out By, Status, and Formats fields unless:
  - The account is disabled. If the account is enabled, then Security Group is displayed above the Checked Out By field. Security Group is displayed above the Account field.
  - The Security Group field is part of a group where it is not the first field, and the lead metadata field has a field order number that positions it above other custom metadata fields. In this case, the Security Group field is displayed in the order that is determined by the field order number of the group's lead metadata field.
- The Release Date and Expiration Date fields are listed as part of the Revision History table at the bottom of the page.
- All other groups with custom metadata fields as the first fields are displayed in the order that is determined by the field order numbers of the lead metadata fields of groups in relation to each other.

The following rules specify how metadata groups are displayed on the Folder Information page.

- The Content ID field is not displayed unless it is part of a group. Currently, any group with Content ID as the first field is not displayed. Counteract this by defining another system or custom metadata field in the group as the lead field.
- All the groups are listed that have system metadata fields as their lead field (provided their assigned display attribute is Edit, Label, or Required). If any system or custom metadata field is assigned a Hidden or Excluded display attribute, it is not displayed.
- All other groups with custom metadata fields as the first fields are displayed in the order that is determined by the field order numbers of the lead metadata fields of groups in relation to each other.

10.4.4 Moving Fields

To force any **custom metadata field** to **display above the Primary File field**:

1. Add the custom metadata field to a group that includes system metadata fields.
2. Make the first field in the group a system metadata field. Group position is based on which system metadata field is the lead field.

To force any **system metadata field** to **display below the Primary File field**:

1. Add the system metadata field to a group that includes custom metadata fields.
2. Ensure that the first field in the group is a custom metadata field.

   The group is displayed below the Primary File field based on the field order number of the lead field.

10.5 Managing Rules

The following tasks are included in rule management:

- Creating, Editing, or Deleting a Rule
- Creating, Editing, or Deleting a Global Rule
- Adding Metadata Fields in a Rule
- Adding, Editing or Deleting Activation Conditions in Rules
- Grouping Metadata Fields
- Custom Conditions and Side Effects
- Setting Default Values, Derived Values and Restricted Lists
- Editing Default or Derived Values and Restricted Lists
- Setting the Display of a Required Field

10.5.1 Creating, Editing, or Deleting a Rule

To create a rule:

1. Use the main menu to choose **Administration** then **Admin Applets**.
2. Click **Configuration Manager** then the **Rules** tab.
3. On the Configuration Manager: **Rules** tab, click **Add**.
4. On the Add/Edit Rule page, click the **General** tab.
5. Enter the name and description information about the new rule.
6. Click **OK**.

To edit a rule, select the rule from the list on the Configuration Manager: **Rules** tab and click **Edit**. Edit the field values and click **OK** when done.

To **delete a rule**, select the rule from the list on the Configuration Manager: **Rules** tab and click **Delete**. Click **OK** to verify the deletion.

10.5.2 Creating, Editing, or Deleting a Global Rule

To create a global rule:

1. Use the main menu to choose **Administration** then **Admin Applets**.
2. Click **Configuration Manager** then the **Rules** tab.
3. On the Configuration Manager: **Rules** tab, click **Add** to create a global rule or highlight a rule and click **Edit** to change a rule to a global rule or edit an existing global rule.
4. On the Add/Edit Rule page, click the **General** tab.
5. Select **Is global rule with priority**.
6. Change the default priority number (optional). By default, 10 is the priority number listed. If editing a rule, change other information as needed. A lower priority rule is executed before higher priority rules which higher priority rules to override the changes made by lower priority rules.
7. Click **OK**.

To **edit a rule**, select the rule from the list on the Configuration Manager: **Rules** tab and click **Edit**. Edit the field values and click **OK** when done.

To **delete a rule**, select the rule from the list on the Configuration Manager: **Rules** tab and click **Delete**. Click **OK** to verify the deletion.

10.5.3 Adding Metadata Fields in a Rule

To add metadata fields to a rule:

1. Use the main menu to choose **Administration** then **Admin Applets**.
2. Click **Configuration Manager** then the **Rules** tab.
3. On the Configuration Manager: **Rules** tab, click **Add** to create a global rule or highlight a rule, and click **Edit** to change a rule to a global rule or edit an existing global rule.
4. On the Add/Edit Rule page, click the **Fields** tab and then click **Add**.
5. On the Add Rule Field page, select the following information:
   - **Display Information Field** check box and **Display Application Fields** check box: if selected, lists metadata fields in the field names list, making fields available for display on standard check-in and search pages.

   Note that if an application field is selected for display in a rule, the field's behavior (as defined for the application that normally uses the field) is changed.
6. Select a field name from the list.
7. Select a general placement choice for the metadata field from the Field Position list for each metadata field added. The selected option adjusts the general placement order of the metadata fields in the list on the Add/Edit Rule page, **Field** tab. The position of each field is relevant to its priority in the evaluation process. You can use the **Up** or **Down** buttons to further refine the placement.
   - **Top**: Moves the metadata field to a relatively higher position.
   - **Middle**: Moves the metadata field to a relatively central position.
   - **Bottom**: Moves the metadata field to a relatively lower position.

8. Click **OK**.
9. On the Add/Edit Rule Field *field_name* page, enter the following display information about each metadata field which determines how the metadata field is displayed on Check In and Search pages:
   - **Edit**: The field is editable even if a default value is provided.
   - **Label**: The field is read-only (fixed but displayed).
   - **Hidden**: The field does not display but when the user submits a content item, this metadata field value remains on the source page.
   - **Excluded**: The field does not display. Unlike a hidden metadata field, an excluded value does not remain on the source page.
   - **Required:** A required field. If this is used, a message is also required.
10. Specify a label for the **Custom Label** field. You can use different labels in different profiles.
11. Use Custom Include: Repositions standard fields. For example, creating a group that includes a placeholder field and the title field moves the title field below the other standard fields on the page. A custom include can then be used for the placeholder field to control how or if it is displayed. Provided files are:

    If selected, allows the use of custom fields. Default: deselected.

    The standard include options listed in the Start Include and End Include lists are defined in the DpDisplayIncludes table of the `std_resources.htm` file. To add additional include options, a custom component must be written defining the new includes and merging them into the DpDisplayIncludes table.
12. Standard Separator: Places a standard horizontal rule on the page where the field otherwise would be.
13. Display Nothing: Hides the field when the page opens.
14. Exclude field from the group count: Prevents the group header from being displayed while keeping the presentation properties of the placeholder field. If the number of fields in a group is greater than zero, then the group header is displayed. For example, a placeholder field used for presentation purposes is the only field in a group that is displayed. Default: deselected.
15. Use Default Value: Allows display of a default value on the Content Check In page or the Search page. Default values are computed for On Request events. You can use Idoc Script, or schema values if the metadata field is associated with a schema view.

    If selected, the **Edit** button is activated and the text pane becomes active, displaying the computed Idoc Script for the field (automatically generated after the default value is added and its properties defined). If unselected, (default), default values cannot be used.
16. Is Derived: Enables the field to be set to a specified value on update or check-in. Values are computed for On Submit and On Import events. You can use Idoc Script, or schema values if the metadata field is associated with a schema view.

    If selected, the **Edit** button is activated and the text pane becomes active, displaying the computed Idoc Script for the field (automatically generated after the value is added and its properties defined). If unselected (default), default values cannot be used.

17. Has Restricted List: Enables the field to be restricted to either a specific list of values or to a filtered list of values.

    If selected, the **Edit** button is activated and the text pane becomes active, displaying the computed Idoc Script for the field (automatically generated after the list is added and its properties defined). If unselected (default), default values cannot be used.

18. Click **OK** when done specifying the attributes of the rule.
19. For each metadata field to be added to the rule, repeat steps 5through 18.

10.5.4 Grouping Metadata Fields

To group metadata fields and add a header to the group:

1. Use the main menu to choose **Administration** then **Admin Applets**.
2. Click **Configuration Manager** then the **Rules** tab.
3. On the Configuration Manager: **Rules** tab, highlight a rule and click **Edit**.
4. On the **General** tab of the Add/Edit Rule page, select **Is group**.
5. Select **Has Group Header**.
6. Click **Edit**.
7. On the Edit Group Header page, provide the following information:
   - **Enable Hiding**: If selected, group metadata fields are hidden and a link appears on the page instead of the fields. Pressing the Show link shows the fields. The default is to display the pages with a Hide link, meaning all fields are displayed by default.
   - **Start and End Include**: Specifies how to display the group. Options include:
     - **Standard Separator**: Inserts a rule above or below the group
     - **Start/End HTML Table**: Displays the group in an HTML table with borders for each row and the header.
     - **Display Nothing**: (default): No distinction is made for the group.
   - **Header Text**: The header string associated with the group of fields.
8. Click **OK** when done.

10.5.5 Adding, Editing or Deleting Activation Conditions in Rules

To add an activation condition to a rule:

1. Use the main menu to choose **Administration** then **Admin Applets**.
2. Click **Configuration Manager** then the **Rules** tab.
3. On the Configuration Manager: **Rules** tab, highlight a rule and click **Edit** to add a condition to a rule or click **Add** to add a new rule.
4. On the Add/Edit Rule page. click the **General** tab then select **Use Rule Activation Condition**.
5. Click **Edit**.
6. On the Add/Edit Rule page, click **Add**.
7. In the dialog, enter the name and click **OK**.

8. Enter the following information using the General pane and Clauses pane. For more information, see Custom Conditions and Side Effects.

   The following options are available on the General pane:

   - **Use Event** check box: If selected, rules can perform differently when events are detected. Events include the following:
     - On Request: Includes an event that results from a user request to view an Content Server page.
     - On Submit: Includes an event that results from a contribution action.
     - On Import: Includes an event that results from a batch loading or archive procedure. The rule is only active for archiver, batch loading, or any other process that uses a special check-in service (for example, Content Publisher).
   - **Use Action**: If selected, rules can perform differently when user actions are detected by the system. User actions include the following (for example, when new contributions are checked in or when a content item is revised):
     - Check in new: Includes the user action of contributing a new content item.
     - Check in selected: Includes the user action of submitting a revision to an item.
     - Content information: Includes the user action of requesting to view the document information page.
     - Content update: Includes the user action of submitting revisions to the document information page.
     - Search: Includes the user action of requesting to view the search page.
   - **Workflow flag**: Enables a rule to perform differently based on the workflow state of a document. For example, when a document is in a workflow, it displays a different Content Information page.

   The following options are available on the Clauses pane. This pane is an Idoc Script wizard used to automate the process of creating Idoc Script statements:

   - Field List: A list of metadata options.
   - Operator List: The method used for searching metadata fields, including the following:
     - Matches: The entire text within the specified metadata field contains the specified metadata Value.
     - Contains Word: The text within the specified metadata field contains the metadata Value.
     - Begins With: The text within the specified metadata field starts with the metadata Value.
     - Is Date Before: The date in the specified metadata field occurs before the Value date.
     - Is Date After: The date in the specified metadata field occurs after the Value date.
   - **Value Field**: You can select an editable field to enter data, a list of options, or an editable field that activates the **Select** button. If the field value is Content ID, pressing **Select** opens the Custom pane. If the field is author, a selection page of users opens.

9. When done configuring the conditions, click **Add** to add the condition to the Clause pane.
10. Click **OK**.

To **edit an activation condition**, follow the previous steps and on the **Conditions** tab, select the activation condition to edit from the list. Edit the field values and click **OK** when done.

To **delete an activation condition**, follow the previous steps and on the **Conditions** tab, select the activation condition from the list and click **Delete**. Click **OK** to confirm the deletion.

10.5.6 Custom Conditions and Side Effects

The **Custom** tab of the Edit Activation Condition page is used to define specific conditions for a rule that, when met, affect the behavior of the profile.

To use this page, click the **Custom** tab then enter customized text in the text pane. Information that is entered is displayed in the text pane on the Add/Edit Rule page.

To define side effects, click the **Side Effects** tab on the Edit Activation Condition page. The Side Effects page is used to:

- Easily add name-value pairs as Idoc Script variables that get pushed to local data using Idoc Script if the activation condition is true.
- Add custom Idoc Script to a rule that is only evaluated if the activation condition is true.

Because the side effect is Idoc Script and evaluated when a rule is activated, you can also include logical statements such as `like if`, `elseif`, and `else`, and can execute any Idoc Script function. For example, you can establish a rule that can control the activation of other rules. For more information about scripting in Idoc Script, see *Developing with Oracle WebCenter Content*.

Add the following information on this page:

- Key: the name used as the Idoc Script variable.
- Value: a literal string that equates to the variable.

Click **Add** when done. The key and value are converted to Idoc Script and are displayed in the editing pane, where you can edit the text.

10.5.7 Setting Default Values, Derived Values and Restricted Lists

To set a default value field or a derived value field:

1. In step 15 or step 16 of the Adding Metadata Fields in a Rule task, select the appropriate check box, then click **Edit**.
2. On the **Conditions** tab, click **Add**.
3. Enter a name for this value attribute and click **OK**.

   The name is added to the Conditions list.
4. Select a Field value and Operator from the lists. Depending on the selected value from the Field list, the Value field provides:
   - An editable field to enter the data.
   - A list of appropriate options.
   - An editable field with a corresponding **Select** button.

5. Enter or select a value for the upper Value field, as applicable:
   a. Click **Select**.

      If the Field value is Content ID, on the Edit Default/Derived Value: Select Field page, select a field for use.

      If the Field value is Author, on the User View page, select a user.

   b. Use the filters to select content. When finished, click **OK**.

   The page closes and the selected content value is added to the upper Value field on the default value **Conditions** tab.
6. Click **Add**.

   The statement is added to the expression pane.
7. Click **Compute**.
8. If the field is linked to a schema view, on the Edit Default/Derived Value: Select Field page, select a column. Otherwise, click **OK**.

   The Select Field page closes and the computed value is added to the lower Value field on the default value **Conditions** tab.
9. Click **OK**.

   The page closes and the Idoc Script statement is displayed in the default value text pane on the Add/Edit Rule Field *field_name* page.
10. If finished adding metadata field attributes, click **OK**. Otherwise, continue to include additional attributes.

To use a restricted list for the metadata field:

1. In step 17 of the Adding Metadata Fields in a Rule task, select **Has Restricted List**. Click **Edit**.
2. To use a list of values directly associated with rules, on the Edit Restricted List page, select **Is Filtered List**. To use a list of specific values, select **Is Strict List** and enter the specific items in the Restricted Value text pane.
3. Click **OK**.

   The Edit Restricted List page closes. If the strict list option is used, the items are displayed in the text pane on the Add/Edit Rule Field *field_name* page.

10.5.8 Editing Default or Derived Values and Restricted Lists

To edit the attributes of a metadata field:

1. Use the main menu to choose **Administration** then **Admin Applets**.
2. Click **Configuration Manager** then the **Rules** tab.
3. On the Configuration Manager: **Rules** tab, click **Add** to create a global rule or highlight a rule and click **Edit** to change a rule to a global rule or edit an existing global rule.
4. On the Add/Edit Rule page, open the **Fields** tab and select the metadata field with attributes to edit. Click **Edit**.
5. On the Add/Edit Rule Field *field_name* page, click the corresponding **Edit** button of the attribute to edit.

6. For either the default value or derived value, select the value to edit in the Conditions text pane.
   a. Select the new Field, Operator or both field values.
   b. To edit the upper Value field value without deleting and redefining the clause, highlight the clause in the Clause pane. Edit the value in the upper Value field, then click **Update**.
   c. Click **Compute**.
   d. Click **OK**.
7. For the restricted list attribute, on the Edit Restricted List page, select the list option and edit the text pane as needed. Click **OK**.
8. Click **OK**.

10.5.9 Setting the Display of a Required Field

Two configuration variables control how required metadata fields appear on the Check In page. For more information, see *Configuration Reference for Oracle WebCenter Content*.

- To use red lettering for a required field, specify:

  ```
  StyleForRequiredFields=requiredField
  ```

- To mark the required field with any symbol, specify:

  ```
  NotationForRequiredFields=*
  ```

  Note: In this example, an asterisk is used to mark the required fields.

10.6 Content Profile Triggers

A *trigger field* is a metadata field defined on the Configuration Manager: **Profiles** tab. If a document matches a *trigger value* for a profile, then that profile is evaluated for the document.

An unlimited number of profiles can exist, but only one trigger value per profile is allowed. For example, if the trigger field is dDocType, *Profile1* can use the trigger value of *ADACCT* and *Profile2* can use the trigger value of *ADSALES*.

The following are true for the selected trigger:

- The trigger field must be a list metadata field. Metadata fields defined as lists are included in the trigger field list.
- After you define the trigger field, you cannot delete it from the system. An Administrator can reset the trigger field to 'none specified', however this disables all profiles.
- If you can change the trigger field, you may invalidate some profiles and have to resolve the situation. User interface hints are provided concerning which profiles are invalid.

> **Note:**
>
> Although you create rules before you create triggers and profiles, it is necessary to know what your trigger is before creating rules.

10.6.1 Selecting a Profile Trigger Field

You can select only one trigger field for each Content Server instance.

To select or change the current profile trigger field:

1. Use the main menu to choose **Administration** then **Admin Applets**.
2. Click **Configuration Manager** then the **Profiles** tab.
3. On the Configuration Manager: **Profiles** tab, click **Select**.
4. On the Edit Trigger Field page, select a new trigger field from the list in the **Field Name** field.
5. Click **OK**.

If you change the trigger field after one or more profiles are created, the new trigger field could cause the existing profiles to become invalid.

10.6.2 Disabling a Profile Trigger Field

To completely disable the trigger field (essentially disabling all profiles as well):

1. Use the main menu to choose **Administration** then **Admin Applets**.
2. Click **Configuration Manager** then the **Profiles** tab.
3. On the Configuration Manager: **Profiles** tab, click **Select**.
4. On the Edit Trigger Field page, select **none specified** from the list in the Field Name field.
5. Click **OK**.

10.7 Creating and Using Content Profiles

This section discusses the tasks involved in creating and using a profile. It covers these topics:

- Creating, Editing, or Deleting a Profile
- Previewing a Profile
- Troubleshooting a Profile

10.7.1 Creating, Editing, or Deleting a Profile

To create a new profile:

1. Use the main menu to choose **Administration** then **Admin Applets**.
2. Click **Configuration Manager** then the **Profiles** tab.
3. On the Edit Trigger Field page, click **Add**.
4. Enter the name of the new profile and click **OK**.
5. On the Add/Edit Profile page, enter the following information:
    - Display label: Specify how the profile is listed in menus.

- Description: brief description of the profile.
- Trigger list: the list values associated with the trigger.
- Exclude non-rule fields: Select to exclude all metadata fields that do not belong to the rules included in the profile.
- Restrict personalization: Select to suppress check in or search links to a particular user or group of users. Idoc Script code based on user information is entered into the Profile Links page and must evaluate to true before a link is displayed. If deselected (default), all links are displayed for all users by default unless evaluated by another profile. Click Edit to customize the list of users.

6. Click **Add** to include rules in the new profile.

> **Note:**
>
> You cannot add rules to the profile until you create and define them using the Configuration Manager: **Rules** tab.

7. On the Add Rule in Profile page, select rules from the list and assign them a general placement priority value.

   Adjust the placement order of the rules in the list by pressing the **Up** or **Down** button. The position of each rule in the list is relevant to its priority in the evaluation process. The general position (top, middle, or bottom) in the list is established when the rule is initially added to the profile. The buttons further refine the placement by moving the rule to a more precise position.

8. Click **OK**.

   The new profile is included in the Profiles list on the **Profiles** tab.

To edit a profile:

1. Select the profile on the Configuration Manager: **Profiles** tab.
2. Click **Edit**.
3. Change the fields as needed.
4. Click **OK**.

To add or edit rules to a profile:

1. Select the profile on the Configuration Manager: **Profiles** tab.
2. Click **Edit**.
3. Click **Add** and select a rule and rule placement from the Add Rule in Profile page.
4. Click **OK** when done.

To delete a profile:

1. Select the profile on the Configuration Manager: **Profiles** tab.
2. Click **Delete**.
3. Click **OK** to verify the deletion.

10.7.2 Previewing a Profile

To preview a profile:

1. Use the main menu to choose **Administration** then **Admin Applets**.
2. Click **Configuration Manager** then the **Profiles** tab.
3. On the Configuration Manager: **Profiles** tab, select the profile to be previewed from the Profiles list.
4. Click **Preview**
5. On the Preview Profile page, select options for use in the profile:
   - Event list: Specifies when an event is included in the profile evaluation.
     - none specified: An event is not included.
     - On Request: Includes an event that results from a user request to view a Content Server page.
     - On Submit: Includes an event that results from a contribution action.
     - On Import: Includes an event that results from a batch loading or archive procedure. The rule is only active for archiver, batch loading, or any other process that uses a special check-in service (for example, Content Publisher).
   - Action list: Specifies when an action is included in the profile evaluation.
     - none specified: A user action is not included in the profile evaluation.
     - Check in new: Includes the user action of contributing a new content item.
     - Check in selected: Includes the user action of submitting a revision to an item.
     - Content information: Includes the user action of requesting to view the document information page.
     - Content update: Includes the user action of submitting revisions to the document information page.
     - Search: Includes the user action of requesting to view the search page.
   - Is workflow list: Specifies when a workflow is included in the evaluation.
     - none specified: A workflow state is not included in the evaluation. The document is or is not in a workflow, but its workflow state is not specified.
     - Yes: The document is in a workflow.
     - No: The document is not in a workflow.
   - Content ID: The content used in the evaluation based on the filter criteria.
   - User Name: The user name used in the evaluation.
6. To review the compiled results of the current profile, do not change any field values on the Preview Profile page. Click **Compute results**.
7. To view the page as an end user sees it, on the Preview Results page, make the following selections:
   - Select **On Request** as the Event field value

- Select an Action value
- Leave the User Name field blank

Click **Show**.

8. Review the computed results and click **OK**.

10.7.3 Troubleshooting a Profile

The Preview Profile page is also used to troubleshoot invalid profiles and perform analysis on any profile.

Troubleshooting using what-if scenarios is an iterative process, composed of trying combinations of inputs to evaluate the profile's rules. In addition to using different input values, you can also use filtered selections of documents.

Changing the different criteria (with or without filters) and computing the results shows how various input combinations affect the evaluation of rules. When the system evaluates the profile's rules, the computed results are displayed either as script string statements (SQL or Idoc Script) in a standard dialog text pane or as simulated Check In or Search pages (if you select On Request as the Event field value). Using the flexibility of the what-if analysis process helps to debug and optimize profiles.

To perform what-if scenarios using diverse combinations of inputs and filters:

1. Select the profile to be reviewed and tested from the Profiles list, and click **Preview**.
2. On the Preview Profile page, select field values, as applicable, from the Event, Action, and Is workflow lists.
3. To include filtered choices for the Content ID field, click the corresponding **Select** button.
4. On the Content Item View page, select content item filter options, as applicable, and click **OK**.
5. To include filtered choices for the **User Name** field, on the Preview Profile page, click the corresponding **Select** button.
6. On the User View page, select user filter options, as applicable, and click **OK**.

To view the evaluated rules as coded statements, on the Preview Profile page click **Compute Results**.

To evaluate results as a simulated page in a browser window, select `Request` in the `Event` field. Select other field values then click `Show` on the Preview Profile page. The system launches a browser window that displays the resulting metadata fields in a simulated Check In or Search page. This window provides a graphic view or what the end user sees.

10.8 Content Profile Examples

The following profile examples illustrate several scenarios in which profiles are useful:

- Department-Based Content Profile (Example)
- Black-Hole Resume Check In (Example)
- Global Rule to Restrict Content Check-In Based on User Role (Example)
- Global Rule Restricting Content Type Metadata Changes (Example)

10.8.1 Department-Based Content Profile (Example)

This example shows how to plan and create a department-based profile that includes one global rule and one regular profile rule.

The goal is to control how the metadata fields governed by the rules are displayed on the Check In, Update, Content Information, and Search pages. Ideally, only department-specific fields are displayed to minimize the number of metadata fields that users see.

This example creates the applicable rules first then the profile because the rules are added to the profile during the process of creating the actual profile. It is divided into the following main steps:

- Create a global rule with the following characteristics:
  - Ensure that all new and updated content items checked in have comments associated with them. The optional comments metadata field is revised to be a required field.
  - Allow the content item title metadata field to be editable.
- Create a profile rule with the following characteristics:
  - Provide a default value for the comments metadata field but also allow it to be editable. The default message is triggered by marketing-specific documents.
  - Provide default values that are read-only text for the publish type and revision label metadata fields.
- Create a department-based profile with the characteristics:
  - Organize the metadata fields that are hidden or displayed on the Check In, Update, Content Information, and Search pages.
  - Display only those fields that are relevant to the marketing department.
  - Group selected metadata fields using a marketing-based group heading.

10.8.1.1 Create the Global Rule

1. Open the **Rules** tab on the Configuration Manager page and click **Add**.
2. On the **General** tab of the Add/Edit Rule page, enter the name of the global rule in the Name field (for example, `CmtsRqd`).
3. Enter a description for the global rule (optional).
4. Select **Is global rule with priority**. You can also change the priority number.
5. Add and define the Comments metadata field as follows:
   a. On the **Fields** tab, click **Add**.
   b. On the Add Rule Field page, select **Comments** from the Field Name list.
   c. Select a general position from the Field Position list (for example, `top`).
   d. Click **OK**.
   e. On the Add/Edit Rule Field *field_name* page, select **Required** from the Type list to ensure that users must enter a comment about the content item being checked in.

f. Enter text in the **Required Message** field. This is optional for all rule field types except the **Required** type.

g. Select **Use default value** and click the corresponding **Edit** button.

h. On the **Conditions** tab of the Edit Default/Derived Value pages, click **Add**.

i. On the Add Condition page, enter the name of the field condition (for example, `UserMsg`).

j. Click **OK**.

k. Enter a short statement in the lower **Value** field, at the far bottom of the page near the **Compute** button. This statement becomes the default value for the **Comment** field.

l. Click **OK**.

m. Click **OK**.

6. Add and define the Document Title metadata field as follows:

a. On the **Fields** tab of the Add/Edit Rule page, click **Add**.

b. Select **Title** from the Field Name list.

c. Select a general position from the Field Position list (for example, `bottom`).

d. Click **OK**.

e. Select **Edit** from the Type list to allow this metadata field to be editable on the Check In and Search pages.

f. Enter a note in the **Required Message** field (optional).

g. Click **OK**.

The **Title** metadata field is added to the Fields list.

7. Click **OK**.

10.8.1.2 Create the Profile Rule

1. Open the **Rules** tab on the Configuration Manager page and click **Add**.
2. On the **General** tab, enter the name of the profile rule in the **Name** field (for example, `DefaultMktComment`).
3. Enter a description for the profile rule (optional).
4. Select **Is group**.
5. Select **Has group header**, and click the corresponding **Edit** button.
6. On the Edit Group Header page, enter the text to use as the header for the grouped metadata fields (for example, `Marketing-Specific Information`).
7. Click **OK**.
8. Add and define the Comments metadata field as follows:

a. On the **Fields** tab, click **Add**.

b. Select **Comments** from the Field Name list.

c. Select a general position from the Field Position list (for example, `top`).

d. Click **OK**.

e. Select **Edit** on the Type list, allowing this field to be editable on the Check In, Update, Content Information, and Search pages.

f. Enter a note in the **Required Message** field (optional).

g. Select **Use default value** and click the corresponding **Edit** button.

h. On the **Conditions** tab, click **Add**.

i. Enter the name of the field condition (for example, `CurrentMktgDocs`).

j. Click **OK**.

k. Enter `These are Current Marketing Docs` into the lower **Value** field at the bottom of the page (near the **Compute** button).

l. Click **OK**.

m. Click **OK**.

9. Add and define the Publish Type metadata field as follows:

a. On the **Fields** tab, click **Add**.

b. Select **Publish Type** from the Field Name list.

c. Select a general position from the Field Position list (for example, `middle`).

d. Click **OK**.

e. Select **Label** from the Type list to make this a read-only field on the Check In, Update, Content Information, and Search pages.

f. Enter a note in the **Required Message** field (optional).

g. Select **Use default value** and click the corresponding **Edit** button.

h. On the **Conditions** tab, click **Add**.

i. Enter the name of the field condition (for example, `MktgDocsOnly`).

j. Click **OK**.

k. Enter **`@dDocName`** into the lower **Value** field at the bottom of the page near the **Compute** button.

l. Click **OK**.

m. Click **OK**.

10. Add and define the Revision Label metadata field as follows:

a. On the **Fields** tab, click **Add**.

b. Select **Revision** from the Field Name list.

c. Select a general position from the Field Position list (for example, `bottom`).

d. Click **OK**.

e. Select **Label** from the Type list to make this a read-only metadata field on the Check In, Update, Content Information, and Search pages.

f. Enter a note in the **Required Message** field (optional).

g. Select **Use default value**.

h. Click **OK**.

11. Click **OK**.

10.8.1.3 Create the Department-Based Profile

1. Open the **Profiles** tab on the Configuration Manager page and click **Select**.
2. On the Add Profile page, select **Type** from the Field Name list.
3. Click **OK**.
4. Click **Add** on the **Profiles** tab.
5. On the Add Profile page, enter the name of the profile (for example, `MktgDoc`).
6. Click **OK**.
7. On the Add/Edit Profile page, enter the profile description in the **Description** field (for example, `Current Mktg docs`).
8. Enter a descriptive label for the profile (for example, `MarketingSpecific`).
9. Select **ADMKT** (or an equivalent marketing option) from the Trigger list.
10. Click **Add** to include the rules in this profile.
11. On the Add Rule in Profile page, select **DefaultMktComment** from the Name list.
12. Select a general priority placement from the Rule Priority list (for example, top).
13. Click **OK**.
14. Click **Add**.
15. Click **OK**.
16. Click **OK**.

    The page closes and the profile is added to the list of profiles on the **Profiles** tab.

10.8.2 Black-Hole Resume Check In (Example)

This example shows how to plan and create a black-hole check in profile used to submit resumes to Human Resources. The goal is to restrict the visible metadata fields available on the Check In, Update, Content Information, and Search pages when using this profile.

After a resume is initially checked in, the derived settings for all the potentially searchable metadata fields prevent unauthorized users from retrieving the document. This example creates the applicable rules first then the profile because the rules are added to the profile during the process of creating the actual profile.

This example is based on the default metadata fields displayed using a non-customized Content Server instance. The visible metadata fields in this profile are limited to Type, Primary File, Alternate File, and Comments. The Type field uses a read-only label. On submission the value is reset to an HR-accessible value to ensure confidentiality of the document. Only the Comments field is editable. The remaining metadata fields are hidden and on submission also have their values reset. In this example, the hidden metadata fields include Title, Author, Security Group, Content ID, Revision, Release Date, and Expiration Date.

If selected, both the Hidden and Excluded display attributes conceal the defined metadata field. Using the Hidden type has the advantage of allowing the field value to remain on the source page. Thus, the contributor does not see the Hidden fields when checking in the document, but the assigned field values are still visible to an authorized viewer. The Excluded type precludes the field values on the source page.

In this type of profile, it is inadvisable to depend on the Exclude non-rule fields check box to hide unnecessary metadata fields. Contributors see only the fields included in the profile's rules, however, it does not prevent default values from being assigned and stored on the source page. Unauthorized users could find a black-hole document by searching on the excluded metadata fields.

This example is divided into the following main steps:

- Create a profile rule that:
  - Hides non-essential metadata fields and does not display them on the Check In, Update, Content Information, and Search pages.
  - Resets the default values of each hidden metadata field to ensure that unauthorized users cannot search and retrieve documents using the hidden fields.
- Create a profile rule that:
  - Allows the display of specific metadata fields related to checking in a resume.
  - Resets the values of each visible metadata field to ensure that unauthorized users cannot search and retrieve documents using these fields.
- Create a black-hole check-in profile that:
  - Restricts the metadata fields that are hidden or displayed on the Check In, Update, Content Information, and Search pages.
  - Displays only those fields that are relevant to an employee who is checking in a resume for an internal company position.

10.8.2.1 Create Rule for Hidden Fields

To create a profile rule for hidden metadata fields:

1. Open the **Rules** tab on the Configuration Manager page and click **Add**.
2. On the **General** tab of the Add/Edit Rule page, enter the name of the rule in the **Name** field (for example, `NoExtraFields`).
3. Enter a description for the global rule (optional).
4. Add and define the **Title** metadata field as follows:
   a. On the **Fields** tab, click **Add**.
   b. On the Add Rule Field page, select **Title** from the Field Name list.
   c. Select a general position from the Field Position list.
   d. Click **OK**.
   e. On the Add/Edit Rule Field *field_name* page, select **Hidden** from the Type list to ensure this metadata field does not appear on the Check In, Update, Content Information, and Search pages.
   f. Enter text in the **Required Message** field (optional).
   g. Select **Is derived field** and click the corresponding **Edit** button.
   h. On the Edit Derived Value: **Conditions** tab, click **Add**.
   i. On the Add Condition page, enter the name of the field condition (for example, `HRsEyesOnly`).

j. Click **OK**.

k. In the lower **Value** field, enter a confidential string (for example, `No specific title`) to help prevent unauthorized users from searching with the **Title** field to retrieve the documents checked in using this profile.

l. Click **OK**.

m. Click **OK**.

5. Add and define the Author metadata field as follows:

a. On the **Fields** tab, click **Add**.

b. Select **Author** from the Field Name list.

c. Select a general position from the Field Position list.

d. Click **OK**.

e. Select **Hidden** from the Type list (to ensure that this metadata field does not display on the Check In, Update, Content Information, and Search pages).

f. Enter text in the **Required Message** field (optional).

g. Select **Is derived field** and click the corresponding **Edit** button.

h. On the **Conditions** tab, click **Add**.

i. Enter the name of the field condition (for example, `HRsEyesOnly2`).

j. Click **OK**.

k. Select **Author** from the Field list.

l. Select **Matches** from the Operation list.

m. Click **Select**.

n. On the User View page, select the applicable user name.

For example, select an HR employee authorized to view the documents checked in with this profile to ensure that unauthorized users cannot search and retrieve these documents using the **Author** metadata field.

o. Click **OK**.

p. Click **Add**.

The clause is added to the clause pane.

q. Click **OK**.

r. Click **OK**.

6. Add and define the Security Group metadata field as follows:

a. On the **Fields** tab, click **Add**.

b. Select **Security Group** from the Field Name list.

c. Select a general position from the Field Position list.

d. Click **OK**.

e. Select **Hidden** from the Type list to ensure that this field does not appear on the Check In, Update, Content Information, and Search pages).

f. Enter text in the **Required Message** field (optional).

g. Select **Is derived field** and click the corresponding **Edit** button.

h. On the **Conditions** tab, click **Add**.

i. Enter the name of the field condition (for example, `HRsEyesOnly3`).

j. Click **OK**.

k. Select **Security Group** from the Field list.

l. Select **Matches** from the Operation list.

m. Select an applicable choice from the Value list. For example, select *HR* or any other department that is authorized to view the documents checked in using this profile.

n. Click **Add**.

o. Click **OK**.

p. Click **OK**.

7. Add and define the Content ID metadata field as follows:

a. On the **Fields** tab, click **Add**.

b. Select **Content ID** from the Field Name list.

c. Select a general position from the Field Position list.

d. Click **OK**.

e. Select **Hidden** from the Type list to ensure that this field does not appear on the Check In, Update, Content Information, and Search pages.

f. Enter text in the **Required Message** field (optional).

g. Select **Is derived field** and click the corresponding **Edit** button.

h. On the **Conditions** tab, click **Add**.

i. Enter the name of the field condition (for example, `HRsEyesOnly4`).

j. Click **OK**.

k. Select **Content ID** from the Field list.

l. Select **Begins With** from the Operation list.

m. Enter a confidential string or click **Select**.

n. On the Select Field page, select a content item from the list. For greater security, enter a unique string (for example, `Res`) to help ensure that unauthorized users cannot search and retrieve these documents using the Content ID metadata field.

o. Click **OK** (if you selected a content item from the Content Item View page).

p. Click **Add**.

q. Click **OK**.

r. Click **OK**.

8. Add and define the Revision metadata field as follows:

a. On the **Fields** tab, click **Add**.

b. Select **Revision** from the Field Name list.

c. Select a general position from the Field Position list.

d. Click **OK**.

e. Select **Hidden** from the Type list (to ensure that this metadata field does not display on the Check In, Update, Content Information, and Search pages).

f. Enter text in the **Required Message** field (optional).

g. Select **Is derived field** and click the corresponding **Edit** button.

h. On the **Conditions** tab, click **Add**.

i. Enter the name of the field condition (for example, `HRsEyesOnly5`).

j. Click **OK**.

k. Select **Revision** from the Field list.

l. Select **Begins With** from the Operation list.

m. Enter a confidential string in the upper **Value** field (for example, `Res`) to ensure that unauthorized users cannot search and retrieve these documents using the Revision metadata field.

n. Click **Add**.

o. Click **OK**.

p. Click **OK**.

9. Add and define the Release Date metadata field as follows:

a. On the **Fields** tab, click **Add**.

b. Select **Release Date** from the Field Name list.

c. Select a general position from the Field Position list.

d. Click **OK**.

e. Select **Hidden** from the Type list to ensure that this field does not appear on the Check In, Update, Content Information, and Search pages.

f. Enter text in the **Required Message** field (optional).

g. Select **Is derived field** and click the corresponding **Edit** button.

h. On the **Conditions** tab, click **Add**.

i. Enter the name of the field condition (for example, `HRsEyesOnly6`).

j. Click **OK**.

k. In the lower **Value** field, enter a confidential string (for example, `No specific release date`) to prevent unauthorized users from using the Release Date field to retrieve the documents checked in using this profile).

l. Click **OK**.

m. Click **OK**.

10. Add and define the Expiration Date metadata field as follows:

a. On the **Fields** tab, click **Add**.

b. Select **Expiration Date** from the Field Name list.

c. Select a general position from the Field Position list.

d. Click **OK**.

e. Select **Hidden** from the Type list to ensure that this field does not display on the Check In, Update, Content Information, and Search pages.

f. Enter text in the **Required Message** field (optional).

g. Select **Is derived field** and click the corresponding **Edit** button.

h. On the **Conditions** tab, click **Add**.

i. Enter the name of the field condition (for example, `HRsEyesOnly7`).

j. Click **OK**.

k. In the lower **Value** field, enter a confidential string (for example, No specific expiration date) to help prevent unauthorized users from using the Expiration Date metadata field to search for and retrieve the documents checked in using this profile).

l. Click **OK**.

m. Click **OK**.

11. Click **OK**.

10.8.2.2 Create Rule for Visible Fields

To create a profile rule for visible metadata fields:

1. On the **Rules** tab, select **Add**.
2. On the **General** tab, enter the name of the profile rule in the **Name** field (for example, `VisibleFields`).
3. Enter a description for the profile rule (optional).
4. Add and define the **Type** metadata field as follows:

   a. On the **Fields** tab, click **Add**.

   b. Select **Type** from the Field Name list.

   c. Select a general position from the Field Position list.

   d. Click **OK**.

   e. Select **Label** from the Type list to make this a read-only metadata field on the Check In, Update, Content Information, and Search pages.

   f. Enter text in the **Required Message** field (optional).

   g. Select **Use default value** and click the corresponding **Edit** button.

   h. On the **Conditions** tab, click **Add**.

   i. Enter the name of the field condition (for example, `ResumeType`).

   j. Click **OK**.

   k. In the lower **Value** field, enter **Resume**.

   l. Click **OK**.

   m. Select **Is derived field** and click the corresponding **Edit** button.

   n. On the **Conditions** tab, click **Add**.

   o. Enter the name of the field condition (for example, `ResumeType2`).

   p. Click **OK**.

   q. In the lower **Value** field, select an appropriate document type from the Value list (for example, `HRresumes`).

r. Click **OK**.

s. Click **OK**.

5. Add and define the Comments metadata field as follows:

a. On the **Fields** tab, click **Add**.

b. Select **Comments** from the Field Name list.

c. Select a general position from the Field Position list.

d. Click **OK**.

e. Select **Edit** from the Type list to allow this metadata field to be editable on the Check In, Update, Content Information, and Search pages.

f. Select **Use default value** and click the corresponding **Edit** button.

g. On the **Conditions** tab, click **Add**.

h. Enter the name of the condition (for example, `PositionAppliedFor`).

i. Click **OK**.

j. In the lower **Value** field, enter an appropriate statement (for example, `Please specify the position title`).

k. Click **OK**.

l. Click **OK**.

m. Click **OK**.

10.8.2.3 Create the Profile

To create the black-hole check-in profile:

1. Open the **Profile** tab on the Configuration Manager page and click **Select**.
2. On the Add Profile page, select **Type** from the Field Name list.
3. Click **OK**.
4. Click **Add** on the **Profiles** tab.
5. On the Add Profile page, enter the name of the profile (for example, `BlackHoleResumeCheckIn`).
6. Click **OK**.
7. On the Add/Edit Profile page, enter the profile description in the **Description** field (for example, `For internal user resumes only`).
8. Select **HRresumes** (or the equivalent option) from the Trigger list.
9. Click **Add** to include the rules in this profile.
10. On the Add Rule in Profile page, select the **NoExtraFields** rule from the Name list.
11. Select a general priority placement from the Rule Priority list.
12. Click **OK**.
13. Click **Add**.
14. Select the **VisibleFields** rule from the Name list.
15. Select a general priority placement from the Rule Priority list.

16. Click **OK**.
17. Click **OK**.

10.8.3 Global Rule to Restrict Content Check-In Based on User Role (Example)

This example illustrates how to create a global rule that can validate metadata fields when users check in content. The global rule validates the data in a request and returns an error message if the data is incorrect. This example shows how to allow only an administrator to check in content that specifies ADACCT as the Content Type.

10.8.3.1 Enable Fatal Error for a Global Rule Violation

1. In a text editor, open the *IntradocDir*`/config/config.cfg` file.
2. Add the following configuration setting:

   ```
   IsDpSubmitErrorFatal=true
   ```

3. Close and save the file.
4. Restart the Content Server.

10.8.3.2 Create Global Rule Restricting Content Type Check-ins

This global rule validates the value for dDocType and ensures that an administrator is checking in an ADACCT document. However, the rule is configured to affect only the Check In and Update pages.

1. Open the **Rules** tab on the Configuration Manager page, and click **Add**.
2. On the **General** tab of the Add/Edit Rule page, enter the name of the global rule in the Name field (for example, `FailOnCheckInError`).
3. Enter a description for the global rule (optional).
4. Select **Is global rule with priority** and change the priority number if needed.
5. Select **Use rule activation condition** and click the corresponding **Edit** button.
6. On the Edit Activation Condition page, click **Add**.
7. On the Add Condition page, enter the name of the condition in the **Name** field (for example, `CheckIn`).
8. Click **OK**.
9. Select **Use event**.
10. Select **On Submit**.
11. Select **Use action**.
12. Select **Check in new**, **Check in selected**, and **Content update**.
13. Click **OK**.
14. Click the **Fields** tab.
15. On the Add/Edit Rule Field *field_name* page, click **Add**.
16. On the Add Rule Field page, select **Type** from the Field Name list.

17. Select a general position form the Field Position list (optional).
18. Click **OK**.
19. On the Add/Edit Rule Field *field_name* page, select **Is derived field** and click the corresponding **Edit** button.
20. On the Edit Derived Value: **Conditions** tab, click the **Custom** tab.
21. On the Custom page, select **Custom** and enter the following Idoc Script:

```
<$if dDocType like "ADACCT" and not userHasRole("admin")$>
<$abortToErrorPage("Only administrators can use ADACCT.")$>
<$endif$>
```

22. Click **OK**.
23. Click **OK**.
24. Click **OK**.

10.8.4 Global Rule Restricting Content Type Metadata Changes (Example)

This example shows how to create a global rule that can validate metadata fields when users check in content. The global rule validates the data in a request, and returns an error message if the data is incorrect. Specifically, this example shows how to allow only an administrator to change the content type of a checked-in document.

10.8.4.1 Enable Fatal Error for a Global Rule Violation

1. In a text editor, open the *IntradocDir*`/config/config.cfg` file.
2. Add the following configuration setting:

```
IsDpSubmitErrorFatal=true
```

3. Close and save the file.
4. Restart the Content Server.

10.8.4.2 Create Global Rule to Restrict Content Type Changes

This global rule validates the value for dDocType and ensures that an administrator is changing the content type of a checked-in document. It is configured to affect only the Check In page.

1. Open the **Rules** tab on the Configuration Manager page and click **Add**.
2. On the **General** tab of the Add/Edit Rule page, enter the name of the global rule in the Name field (for example, `FailOnCheckInError`).
3. Enter a description for the global rule (optional).
4. Select **Is global rule with priority** and change the priority number if needed.
5. Select **Use rule activation condition** and click the corresponding **Edit** button.
6. On the Edit Activation Condition page, click **Add**.
7. On the Add Condition page, enter the name of the condition in the Name field (for example, `CheckIn`).
8. Click **OK**.
9. Select **Use event**.

10. Select **On Submit**.
11. Select **Use action**.
12. Select **Content update**.
13. Click **OK**.
14. Click the **Fields** tab.
15. Click **Add**.
16. On the Add Rule Field page, select **Type** from the Field Name list.
17. Select a general position form the Field Position list.
18. Click **OK**.
19. On the Add/Edit Rule Field *field_name* page, select **Is derived field** and click the corresponding **Edit** button.
20. On the Edit Derived Value: **Conditions** tab, click the **Custom** tab.
21. On the Custom page, select **Custom** and enter the following Idoc Script:

```
<$oldType =getValue("DOC_INFO", "dDocType")$>
<$newType =getValue("#local", "dDocType")$>
<$if not (newType like oldType) and not (userHasRole("admin"))$>
<$abortToErrorPage("Only administrators can change dDocType.")$>
<$endif$>
```

22. Click **OK**.
23. Click **OK**.
24. Click **OK**.

Part IV
Managing Records

This section of the documentation describes the Oracle WebCenter Content: Records functionality.

Managing Records contains the following chapters:

- Configuring Records Management
- Managing a Records Retention Schedule
- Managing Security for Records
- Defining and Processing Dispositions
- Managing the Oracle WebCenter Content Records Adapter
- Managing Physical Content
- Processing Reservations and Chargebacks
- Configuring Related Content (Links) for Records
- Managing the Records System
- Using Federated Search and Freeze

> **Note:**
>
> All metadata field descriptions for each action are available in *User Help for Oracle WebCenter Content (Native 11g UI)* available within the WebCenter Content Native UI. Also, see Creating Records and Physical Content in *Using Oracle WebCenter Content* for additional information.

11

Configuring Records Management

This chapter provides configuration information on the Records portion of Oracle WebCenter Content, which is used to manage content items on a retention schedule.
The focus of *records management* tends to be the preservation of content for historical, legal, or archival purposes while also performing retention management functions. The focus of *retention management* tends to be the scheduled elimination of content based on a schedule designed by a record administrator. Both records and retention management are combined to track and preserve content as needed, or dispose of content when it is not longer required.

> **Important:**
>
> You must configure all defaults, including any necessary categories, dispositions, and triggers, before checking in content that will use those defaults.

Items for retention are any form of information, both physical and electronic, that is important enough for an organization so it must be retained for a specific period and may be disposed of when no longer needed. However, information can be revisioned, retained, and managed on a disposition schedule. An organization may choose to manage content to eliminate outdated and misleading information and track documents related to legal proceedings.

This chapter covers the following topics:

11.1 Understanding Records Management

Many organizations are subject to regulations that require the retention of information for a specified period:

- Sarbanes Oxley:
  - Applies to all publicly traded corporations or companies that may become public

  - Audit-related working papers, communications, and correspondence must be retained for five years after the audit
- Government organizations: DoD 5015.2, General Records Schedule
- Pharmaceutical/health care industry: HIPAA, FDA regulations
- Financial services: SEC Rule 17a
- Telecommunications industry: 47 CFR 42, and so on

There may be litigation-related needs for effective and efficient retention management:

- Policy-based retention of content:
  - Retain information needed for litigation (for example, a contract and any communication relating to it).
  - Centralized searching and retrieval of that information.
- Systematic disposition of eligible content:
  - Less material to search through during discovery.
  - Less material to give to opposing counsel.
- Suspend/freeze disposition of content relating to pending litigation:
  - Avoid appearance of cover-up and possible liability when content relating to pending litigation is destroyed.

There may be business-related needs for effective and efficient retention management:

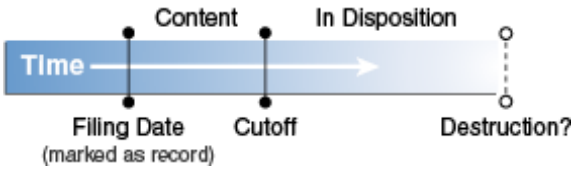
- To organize items that are created in a variety of forms (email, CDs, DVDs) and which are stored in a variety of locations (employee computers, central file storage, and so on).
- To provide a uniform infrastructure for retrieving and sharing the content across the organization.:
- The information may be required for the day-to-day operations of the organization and must be kept for historical, tracking, or audit purposes (for example, receipts, order histories, completed forms, personnel files, corporate announcements).
- The information may be necessary to the success or survival of the organization (for example, software source code, contracts, financial data).
- There may be internal policies or external regulations requiring the information to be retained (for example, transaction documents, financial statements, lease agreements).
- To ensure that content items are retained over the period they are useful to the business.

This section discusses the following additional topics in records management:

11.1.1 Life Cycle for Retained Content

The life cycle of retained content goes through several stages.

Figure 11-1 Life Cycle of Retained Content



The **filing date** is the date a content item is marked as an item being tracked. This often coincides with the check-in date. However, it is possible for an active content item already checked in to be tracked.

The information may need to be for different periods of time, depending on the type of content, its use within the organization, and the need to comply with external laws or regulations.

The **cutoff** of a content item is the moment the status of the item changes and the item goes into disposition. An item may be cut off after a specific period, at a specific event, or after an event.

Items are disposed of by authorized people according to the requirements of the organization. Disposition actions can include destruction, storage, transfer, or an item can be deemed so important it will never be destroyed (for example, due to historical significance). "Disposal" in this instance indicates a status changes from active use.

A life cycle can be explicitly defined. See Configuring Retention Definitions and Options.

11.1.2 Types of Retained Content

Retained content can be divided into categories depending on the perspective:

- Internal and External Retained Content
- Classified_ Unclassified_ Declassified Content
- Non-Permanent_ Transfer or Accession_ and Reviewed Content

11.1.2.1 Internal and External Retained Content

An *internal* retained content item is an electronic item stored within Oracle WebCenter Content and managed by the product.

External content can also be managed. An *external* retained content item is a source file not stored in Oracle WebCenter Content. It can be in a variety of formats, both physical or electronic. The software can manage the disposition schedule, search metadata associated with the external file, and manage an electronic rendition of an external file. An electronic rendition can either be checked in as a primary file of an external item, or be filed as a separate file, and then linked to the external file metadata.

11.1.2.2 Classified, Unclassified, Declassified Content

Content can be *classified*, *unclassified*, or *declassified*.

- **Classified** content is that which requires protection against unauthorized disclosure (for example, because it contains information sensitive to the national security of the United States or because it is essential for a corporation's operation).
- **Unclassified** content is not and has never been classified.
- **Declassified** content was formerly classified, but that classified status has been lifted.

A *classification* specifies the security level of a classified content item. A *classification guide* provides default classification values for check-in pages.

Options can be chosen during the initial setup to insure that the system complies with the DoD 5015.2 standard (including Chapter 4). The software has been certified by the Joint Interoperability Test Command (JITC) to comply with that standard. A copy of the standard is available on the official website of the Department of Defense, Washington Headquarters Services, Directives and Records Division at `http://www.dtic.mil/whs/directives/`.

> **Important:**
>
> Executive Order 12958: Classified National Security Information describes in detail the system for classifying, safeguarding, and declassifying national security information. This guide assumes you are familiar with proper classification protocols.

11.1.2.3 Non-Permanent, Transfer or Accession, and Reviewed Content

For disposition purposes, content is categorized into *non-permanent*, *transfer or accession to NARA*, and *subject to review*. Most items fall into the non-permanent category.

Non-permanent items are usually destroyed after a retention period. Permanent items are deemed important for continued preservation and are retained indefinitely (for example, because of their historical significance).

Items can be scheduled for periodic reviews by authorized people. This complies with the DoD Vital Record Review criteria.

11.1.3 Basic Retention Management Concepts

Records is used to manage content, regardless of source or format, in a single, consistent, manageable infrastructure. Managed items are assigned retention schedules and disposition rules that allow users to schedule life cycles for content to eliminate outdated or superseded information, manage storage resources, or comply with legal audit holds.

Content and its associated metadata are stored in retention schedules, which are hierarchies with categories that define disposition instructions. Access to the items is

controlled by rights assigned to users by a Records Administrator. The items can be accessed, reviewed, retained, or destroyed in an easy and efficient manner by authorized people according to the requirements of an organization.

Disposition schedules of content in the repository can also be managed, enabling the scheduling of life cycles for content to eliminate outdated or superseded information, manage storage resources, or comply with legal audit holds.

The following concepts are important to understand in the context of retention management:

- **Record administrator**: individuals in the organization who are responsible for setting up and maintaining the retention schedule and other aspects of the management system.
- **Record user**: individuals who use the software to check content in and out of the system, to search for records, and to perform other non-administrative tasks.
- **Record officer**: individuals who have limited administrative responsibility in addition to the responsibilities of a record user.
- **Administrator**: individuals who may maintain the computer system, network, or software at the site where the management system is in place.
- The **retention schedule** is an organized hierarchy of series, categories, and record folders, which allows users to cluster retained content into similar groups, each with its own retention and disposition characteristics.
- A **series** is an organizational construct in the retention schedule that assists in organizing categories into functional groups. Series are normally static and are used at a high level in an organization hierarchy. They can be especially useful if a large amount of categories are used. A series can be nested, which means a series may contain other series.
- A **retention category** is a set of security settings and disposition instructions in the retention schedule hierarchy, below a series. It is not an organization construct but rather a way to group items with the same dispositions. A category helps organize record folders and content into groups with the same retention and disposition characteristics. A retention category may contain one or more record folders or content items, which then typically follow the security settings and disposition rules associated with that retention category. Retention categories *cannot* be nested, which means a retention category cannot contain other retention categories.
- A **record folder** is a collection of similar content items in the retention schedule. Folders enable content to be organized into groups. A folder typically follows the security settings and disposition rules associated with its assigned retention category. Folders can be nested, which means a folder may contain other folders.
- **Disposition** is the collective set of actions taken on items. Disposition actions include wait times and activities such as transfer to external storage facilities, the destruction of temporary content, deletion of previous revisions, and deletion of all revisions.
- A **disposition instruction** is created within a retention category, and typically consists of one or more disposition rules, which define how content is handled and what actions should be taken (for example, when and how content should be disposed of).
- A **period** is the segment of time that must pass before a review or disposition action can be performed. Several built-in periods are provided (for example, "one year"), but custom periods can be created to meet unique business needs.
- A **trigger** is an event that must occur before a disposition instruction is processed. Triggers are associated with disposition rules for retention categories. Examples of triggering events include changes in status, the completed processing of a preceding disposition action, or a retention period cutoff.

- A **link** is a defined relationship between items. This may be useful when items are related and need to be processed together. Links are available for items stored both in and out of the retention schedule.
- A **classification** specifies the security level of a classified item. It is used in the process of identifying and safeguarding content containing sensitive information. Typical classification levels are "Top Secret," "Secret," and "Confidential," and "Unclassified."
- A **classification guide** is a mechanism used to define default values for several classification-related metadata fields on the content check-in pages for content. A guide enables convenient implementation of multiple classification schemes.
- **Freezing** inhibits disposition processing for an item. Frozen content cannot be altered in any way nor can it be deleted or destroyed. This may be necessary to comply with legal or audit requirements (for example, because of litigation). Freezing is available for items stored both in and out of the retention schedule.
- **External items** are those that are not searched and processed in the same fashion as retained content. External content usually refers to content managed by Physical Content Management or managed by an adapter (an add-on product).
- **Federation, Federated Search, Federated Freeze** are functionality used to manage the process of legal discovery. Using Federated Search or Freeze, a legal officer can search content across all repositories to gather information needed for legal proceedings.

11.1.4 Physical Content Management

Physical Content Management (PCM) provides the capability of managing physical content that is not stored in the repository in electronic form. All items, internal and external regardless of their source or format, are managed in a single, consistent, manageable infrastructure using one central application and a single user interface. The same retention schedules are used for both electronic (internal) and physical (external) content.

PCM tracks the storage locations and retention schedules of the physical content. The functionality provides the following main features:

- **Space management**, including definition of warehouse layout, searching for empty space, reserving space, and tracking occupied and available space.
- **Circulation services**, including handling reservation requests for items, checking out items, and maintaining a due date for checked-out items.
- **Chargeback services**, including invoicing, for the use of storage facilities and/or actions performed on physical items.
- **Barcode file processing**, including uploading barcode information directly into the system, or processing barcode files manually.
- **Label creation and printing**, including labels for users, storage locations, or individual physical items.
- **Retention management**, including periodic reviews, freezes and litigation holds, and email notifications for pending events.

11.1.5 Basic Retention Processes

The following steps outline the basic workflow of retained content:

1. The retention schedule and any required components, such as triggers, periods, classifications, and custom security or metadata fields are created.
2. Items are filed into the retention schedule by users. The filed items assume the disposition schedules of their assigned category.
3. Disposition rules are processed in accordance with the defined disposition schedules, which usually have a retention period. The processing is activated by either a system-derived trigger or custom trigger. The trigger could affect one or more items simultaneously.
4. Whenever a disposition event is due for action (as activated by a trigger), an e-mail notification is sent to the person responsible for processing the events. The same is true for review. The pending events and reviews are displayed in the pages accessed from the Retention Assignments links within the user interface.
5. The Records Administrator or privileged user performs the review process. This is a manual process.
6. The Records Administrator processes the disposition actions on the pending dispositions approval page. This is a manual process.
7. A batch process is run to process an approval.

Many disposition schedules are *time-based* according to a predictable schedule. For example, content is often filed then destroyed after a certain number of years. The system tracks when the affected content is due for action. A notification email is sent to reviewers with links to the pages where reviewers can review and approve content and folders that are due for dispositions.

In contrast, *time-event* and *event-based* dispositions must be triggered with a non-system-derived trigger (a trigger that was defined for a particular scenario). For example, when a pending legal case starts litigation, the Records Administrator must enable the custom trigger and set its activation date because the start date information is external. Custom triggers can define event and time-event based disposition actions based on the occurrence of a particular event.

11.2 Selecting the Software Configuration

By choosing certain options, specific components are enabled and ready for use. To view details about the components that are installed and the disposition actions enabled with each option, click the *i* button next to the option.

The following options are available to enable:

- **Folders Retention**: Enables functionality to apply retention rules for deletions of items stored together in a retention query folder. See Managing a Records Retention Schedule for a summary of this feature.
- **Minimal**: Enables the minimal amount of functionality and excludes some disposition actions and most of the application features. This is the default when the software is enabled.
- **Typical**: Enables all disposition actions and all features except for DoD Configuration, Classified Topics, and Email.
- **DoD Baseline**: Enables the features from a Typical installation with the addition of DoD Configuration and Email.
- **DoD Classified**: Enables all features.

- **Custom**: Enables the ability to choose a variety of features. Some disposition actions are dependent on other actions. If an action is selected, dependent actions are also automatically selected.

To set the software configuration:

1. Choose **Records** then **Configure** then **Enabled Features**.
2. On the Enabled Features page, select the type of configuration. After selection, the feature and disposition options at the bottom of the page appear with the check box selected, indicating which choice is included. If **Custom** is selected, choose which features and dispositions to be enabled.
3. Click **Submit**.

> **Important:**
>
> You must configure all defaults, including any necessary categories, dispositions, and triggers, before checking in content that will use those defaults.

If DoD functionality is enabled by using either DoD option (or a customized option that enables DoD features), then some features are automatically enabled as well. For example, when creating custom search templates, the Security Classification status of a content item is always displayed whether or not the classification was chosen for inclusion in the template. It is a requirement of the DoD specification that the classification level always be displayed in a search result.

After making selections or changing options (for example, switching from Baseline to Classified), restart Content Server. Depending on the search options are in use, the index may also need to be rebuilt. For details about restarting the system and rebuilding the index, see *Administering Oracle WebCenter Content*..

If a component is disabled, the data used with that component is not deleted. If the component is enabled again, the old data can still be used.

11.2.1 Usage Notes

Depending on the cache settings for your browser, it may need to be restarted or the cache settings must be cleared in order to view changes made to the configuration. For example, if you enable Offsite Storage functionality, you may need to clear the cache settings and restart your browser for the appropriate options to appear on the **Physical** menu. The same is true if you disable functionality in order to remove the options.

When using Records with a Safari browser, menus can appear behind the icons for the Admin Applets. Therefore, if you choose **Administration** then **Admin Applets** then choose **Records** or **Physical**, the options on the **Records** or **Physical** menu appear behind the icons for the Admin Applets. This is a known problem and Oracle is working to solve this issue.

11.3 Retention Management Options

After choosing the features to use, certain options must be configured in order for the system to work properly. If not done, a warning messages appears indicating that the setup is incomplete.

To complete the configuration, click the link in the warning message. The Setup Checklist page opens showing a series of links to other pages where configuration selections can be made. When done configuring, select the check box next to an option to indicate the completed task. Depending on the action, it may be necessary to refresh the frame in order to view the completed tasks.

The Setup Checklist can also be accessed by choosing **Records** then **Configure** then **Setup Checklist**.

All defaults, including any necessary categories, dispositions, and triggers, must be set before checking in content that will use those defaults.

> **Important:**
>
> If File Store Provider is needed to check in templates, set up the File Store Provider first and then check in the templates. To install a file store provider, click **Install Default Templates (Category Defaults, Reports, Dashboards, etc.)** on the Setup Checklist page. For details about using File Store Provider, see *Administering Oracle WebCenter Content*.

If the configuration of the system changes (for example, switch from DoD Baseline to Typical) reconfigure the options needed for the level of functionality that is enabled.

The required options include:

- Set configuration variables: Several optional variables can be changed.
- Define default metadata: Some content items are automatically checked in to the repository such as audit entries and screening reports. In order for them to check in properly, choose default metadata for the content. For example, if a DoD installation level is chosen then the default metadata must include the *Category or Folders* metadata field.
- Configure the installation: Before using the system, complete the installation steps outlined in Selecting the Software Configuration.
- Configure the security settings: Determine the appropriate roles, rights, and user permissions to perform certain tasks.

The other configuration options on this page can be performed in any order. When finished setting configuration options, click **Submit**. To clear the options selected, click **Reset**.

The following list provides an overview of the steps needed to set up the retention software. The steps should be followed in the order given. For example, you must define triggers and periods before disposition rules, because when you define a category and its disposition rule, you include references to triggers and periods.

> **Tip:**
>
> To track actions while setting up and configuring the system, first configure the audit trail. All user actions are set to be recorded by default.

Some of these tasks may be optional depending on your organization. The information is provided so you can determine if the step may be useful.

- Determine additional security settings.
- Configure system settings:
  - Set the calendar for the organization. See Setting the Fiscal Calendar.
  - Define the time periods associated with retention or disposition of retained content.
  - Set up any custom fields required.
- Set up the retention schedule. This includes:
  - Managing the methods of grouping content in a retention schedule. For details, see Using a Series, Managing Retention Categories, and Managing Record Folders.
- Determine how content will be handled:
  - Using triggers to initiate events affecting content. For details, see Working with Triggers.
  - Defining the sequence of actions to be performed on items during their life cycle. For details, see Creating Dispositions.
  - Inhibiting disposition processing. For details, see Managing Freezes.
- Establish relationships between content. For details about establishing links between content items, see *Using Oracle WebCenter Content*.

11.4 Setting Up Physical Content Management

Several aspects of PCM should be set up in order to use the system. These include:

- Set up the required PCM user roles and rights.
- Configure the PCM environment including chargebacks, customers, and object types. See Managing Physical Content.
- Define the storage space environment. See Configuring Storage Space.
- Define disposition rules for physical content, if required. See Defining and Processing Dispositions.

11.5 Configuring Retention Definitions and Options

Several system-wide configuration settings are specified on the Configure Retention Settings page. Most of these options can be set by selecting the check box next to the option. General configuration choices are available by choosing **Records** then **Configure**. Choose **Settings** to open the Configure Retention Settings page.

General options:

- Start of fiscal calendar: Sets the start date for the calendar used for fiscal accounting. See Setting the Fiscal Calendar.
- Archive Metadata Format: Sets the storage file format for metadata of items in a disposition bundle.
- Log Metadata Changes: Enables tracking of item-level metadata changes.
- Enable Category Dispositions Review: Enables the workflow to review category dispositions. The workflow must be set up before this option is enabled.
- Enable Report Exclude Search Options: Enables an option that allows a user to exclude reports from searches.
- Lifecycle Start Time: Sets the start time for computing and updating disposition rules. If the same value is used for the start and end times, processing occurs 24 hours per day.
- Lifecycle End Time: Sets the end time for computing and updating disposition rules. If the same value is used for the start and end times, processing occurs 24 hours per day.
- Vital Start Time: Sets the start time for computing and updating vital record review requirements. If the same value is used for the start and end times, processing occurs 24 hours per day.
- Vital End Time: Sets the end time for computing and updating vital record review requirements. If the same value is used for the start and end times, processing occurs 24 hours per day.

Record Definition options:

- Always restrict revisions/Never restrict revisions: Allows revisions of content items or prevents revisions.
- Always restrict deletions/Never restrict deletions: Allows deletions of content items or prevents deletions.
- Always restrict edits/Never restrict edits: Allows edits of content or prevents content editing.
- Display record icon when: Indicates when a record icon should be shown. Options include when editing, deleting, or revisioning of content is restricted or any combination of those actions. The appearance of the record icon can also be disabled. The icon can assist users to determine the status of content (that is, if it is considered a record for tracking purposes).

Security options:

- ACL-based security: Enables security on Retention Schedule objects based on Access Control Lists.
- Default Oracle WebCenter Content security on Retention Schedule objects: Enables default security on categories, folders, and triggers.
- Supplemental Markings: Enables supplemental marking security on retention objects.
- User must match all supplemental markings: Forces a user to match all markings to access an item.
- Custom security fields: Enables the ability to create custom security fields.
- Classified security: Enables classified security features (required for conformance to the Chapter 4 Classified Records section of the DoD 5015.2 specification).

Notification options:

- Do not notify authors: Prevents email notifications to be sent for pending events, reviews, and the Notify Authors disposition action.

Scheduling options:

- Only allow scheduled screening: Prevents users from starting screenings manually by hiding the **Search** button on the screening page.

User interface options:

- User-friendly disposition: Enables user-friendly language for disposition rules and processing.
- Show export date: Enables users to export items that changed since a specific date.
- Use page Navigation: Displays more elaborate page navigation controls on screening results lists and record folder lists.
- Paginate Navigation Tree: Displays the retention schedule in the **Browse Content** menu as a tree-like structure when using the Trays layout. If more than 20 items are available for viewing, an option appears to view the next 20 items in the structure.

DoD Configuration options:

- Enable custom scripting: Allows creation of custom scripts for security or for notifications.

Classified topic options:

- Run auto computation of declassification date: Computes the declassification date for classified objects.
- Maximum years before declassifying: Sets the number of years after which content is declassified.

11.5.1 Setting the Fiscal Calendar

> **Important:**
>
> The Admin.RecordManager right is required to perform this task. This right is assigned by default to the Records Administrator role.

The fiscal calendar is the calendar used by an organization for financial and accounting purposes. A fiscal year may coincide with a calendar year (that is, run from January 1 to December 31), but that is not required.

Specify the start date of the fiscal year once, unless the organization changes the fiscal start date or the start date varies from year to year. The fiscal start date may need to be set manually each year if your organization has a unique fiscal calendar start, such as the first Monday of each year, for example, because a date does not fall on the same weekday each year.

To set the fiscal calendar start date:

1. Choose **Records** then **Configure** then **Settings**.

2. On the Configure Retention Settings page, specify the date the fiscal year begins for the organization in the **Start of Fiscal Calendar** box. To enter a date, enter the starting date and select the month from the list. For example, if your organization starts its fiscal calendar on April 1, type `1` and select `April` from the list of months.
3. Click **Submit Update**.

   A message appears saying the configuration was successful.
4. Click **OK**.

11.5.2 Managing Time Periods

Periods define a length of time to use in retention schedules and dispositions. They are associated with retention periods for dispositions and with review periods for cycling subject-to-review content.

Three types of time periods are used in retention:

- Custom: A custom period has a defined start date and time usually not corresponding to a fiscal or calendar year period.
- Fiscal: A fiscal period corresponds to a fiscal year.
- Calendar: A calendar period corresponds to the calendar year.

Built-in periods cannot be edited or deleted. A user can edit any periods that are created, and created periods can be deleted if the period is not in use.

To work with periods, the following rights are required:

- Admin.Triggers: This right enables a user to view information about periods.
- Admin.RecordManager: In addition to viewing information about periods, this right also enables a user to create (add), edit, and delete periods.

The following calendar periods are predefined:

- Calendar Quarters (wwRmaCalendarQuarter)
- Calendar Years (wwRmaCalendarYear)
- Months (wwRmaMonth)
- Fiscal Quarters (wwRmaFiscalQuarter)
- Fiscal Halves (wwRmaFiscalHalves)
- Fiscal Years (wwRmaFiscalYear)

Weeks (wwRmaWeekEnd) are defined as a built-in custom period.

The following tasks are performed when managing time periods:

- Creating or Editing a Custom Time Period
- Viewing Period Information
- Viewing Period Usage
- Deleting a Custom Period
- Example: Creating a Custom Period

11.5.2.1 Creating or Editing a Custom Time Period

This section provides information on how to create or edit a custom period.

> **Note:**
>
> The Admin.RecordManager right is required to perform this action. This right is assigned by default to the Records Administrator role.

Custom periods can be created in addition to the standard calendar periods already defined. For example, you may need a calendar period such as decade or century for the review cycle or retention period needs of your organization.

11.5.2.1.1 Creating a custom period

To create a custom period:

1. Choose **Records** then **Configure**.
2. Choose **Retention** then **Periods**.
3. On the Configure Periods page, click **Add.**
4. On the Create or Edit Period page, enter a name for the period.
5. Select the type of time period, either Calendar, Fiscal, or Custom. The start date of the fiscal year is defined on the Configure Retention Settings page. The Custom option is useful for creating lengthy periods such as decades or centuries, or unusual periods such as School Year Session, or Software Development Cycle.
6. Click the calendar icon and select or edit a custom start time.
7. Enter an integer value for the length of the time period and choose a time unit from the Length list.
8. Enter a label to describe the end of the period.
9. Click **Create**.

   A message appears saying the period was created successfully, with the period information.
10. Click **OK**.

11.5.2.1.2 Editing a time period

To edit a time period:

1. Choose **Records** then **Configure**.
2. Choose **Retention** then **Periods**.
3. On the Configure Periods page, choose **Edit Period** from the item's **Actions** menu for the period to edit.
4. On the Create or Edit Period page, edit the appropriate information.
5. Click **Submit Update.**

A message appears saying the period was updated successfully.

6. Click **OK**.

11.5.2.2 Viewing Period Information

> **Note:**
>
> Either the Admin.Triggers or Admin.RecordManager right is required to perform this action. The Admin.Triggers right is assigned by default to the Records Administrator and Records Officer roles and the Admin.RecordManager right to the Records Administrator role.

To view information about a period:

1. Choose **Records** then **Configure**.
2. Choose **Retention** then **Periods**.
3. On the Configure Periods page, click the period to view from the **Period Name** list.

   The Built-in label indicates if a period was predefined. A period created by an administrator always displays No for the Built-in label. If a period is a built-in period, the **Edit** option is not displayed on the page because a user cannot edit a predefined period. The **Actions** menu is not available to any users other than those with the Admin.RecordManager right.
4. When done, click **OK**.

11.5.2.3 Viewing Period Usage

> **Note:**
>
> Either the Admin.Triggers or Admin.RecordManager right is required to perform this action. The Admin.Triggers right is assigned by default to the Records Administrator and Records Officer roles. The Admin.RecordManager right to the Records Administrator role.

Period usages are usually viewed to determine why a custom period cannot be deleted.

To view period references:

1. Choose **Records** then **Configure**.
2. Choose **Retention** then **Periods**.
3. On the Configure Periods page, click the period to view from the list.
4. Choose **References** from the Information page **Actions** menu.

   The Period Reference page opens. This page shows all folders, categories, and/or category dispositions the current period is referenced by, with a link to each of the referencing items. If a link is clicked, the associated information page for the item opens.
5. When done, click **OK**.

11.5.2.4 Deleting a Custom Period

> **Note:**
>
> The Admin.RecordManager right is required to perform this action. It is assigned by default to Records Administrator role.

Built-in periods cannot be deleted. Before deleting a period, verify that the period is not referenced by a retention period within a disposition rule for a category, or by a review period for an item, record folder, or retention category.

1. Choose **Records** then **Configure**.
2. Choose **Retention** then **Periods**.
3. On the Configure Periods page, choose **Delete Period** from a period's **Actions** menu.

   A message appears saying the period was deleted successfully.
4. Click **OK**.

11.5.2.5 Example: Creating a Custom Period

This example demonstrates creating a custom period with the following characteristics:

- The custom period name is School Year 2010-2011.
- The custom start time is September 7th, 2010, and the start time is 9:00 am. The system automatically calculates and tracks the end of the period.
- The length of the period is nine months.
- The end of the period label is End of School Year 2011.

To create a custom school period:

1. Choose **Records** then **Configure**.
2. Choose **Retention** then **Periods**.
3. On the Configure Periods page, click **Add** in the Period Name area.
4. On the Create or Edit Period page, enter `School year 2010-2011` as the Period Name.
5. By default, the **Custom** option is already selected in the Period Type list. Leave the Custom option selected.
6. Click the calendar icon and select a custom start date of `September 7, 2010`. The date and default time show in the **Custom Start Time** box. The time defaults to 12 am (midnight) on this page, so to edit the time, you must do so directly in the Custom Start Time text box. Change `12` to `9`. Specify the date according to the format used by your system locale.
7. Enter `9` as the Length and select Months from the list.
8. Enter `End of School year 2010-2011` as the label for end of period.

9. Click **Create**.

   A message appears saying the period was created successfully.

10. Click **OK**.

11.5.3 Setting Performance Monitoring

Performance monitoring can be enabled to check the status of batch processing, service calls, and other system information. To enable this, choose **Records** then **Audit**. Choose **Configure** then **Performance Monitoring**.

Several default numbers have been set as a starting point for monitoring. Actual performance variations will depend on the hardware used at the site and other variables such as total amount of content and software in use.

For details about using performance monitoring, see *Administering Oracle WebCenter Content*.

11.6 PCM Options

Some general configuration options for Physical Content Management are available on the Configure Retention Settings page. This is similar to the Configure Retention Settings page where a series of options are used to determine system functionality.

To access this page, choose **Physical** then **Configure** then **Settings**. Other configuration options are available on the **Configure** menu, such as setting up chargebacks, invoices, and other aspects of Physical Content Management.

The following options appear on the Configure Physical Settings page:

- Default Transfer Method: Specifies the default transfer method (copy, fax, mail, and so on).
- Default Request Priority: Specifies the default priority to be used for reservations (no priority, rush, this week, and so on).
- Default Checkout Period (days): Specifies the number of days a reserved physical item can be checked out.
- Delete completed requests: Specifies if completed reservation requests are automatically deleted after a specified number of days.
- Request history period (days): The maximum number of days a reservation request is stored in history.
- Check in internal content item for reservation workflow: Specifies if a new internal content item should be checked in when a reservation request is made.
- Do not notify users when checked-out items are overdue: Specifies that users with late items receive an email notification.
- Allow reservation requestors to modify/delete their reservations: Specifies if users who create a reservation request can modify or delete their open requests.
- Automatically update request waiting list: Specifies if waiting lists for requests are updated automatically.
- Show batch services: Specifies if batch services are available in the **External Content** menu.

- Enable offsite functionality: Specifies if the storage of content offsite is enabled. When this is enabled, new metadata fields are added to the system as well as the Offsite security group.

11.7 Creating Custom Metadata Sets

If an organization has unique needs for metadata fields for retention categories or record folders, the software can be customized to include the fields. Depending on the field characteristics, the new custom fields are displayed on the Create Category, Create Folder page, or Create Physical page (if Physical Content Management is enabled). These fields are also displayed on the edit and information pages for those retention schedule objects.

The order in which the custom metadata fields appear depends on the order indicated in the custom metadata fields box. The fields can be arranged using the arrows near the custom metadata box.

Custom fields can be added to existing tables already in use in the repository. These fields supplement the fields uses with retention category pages, record folder pages, and physical items pages.

Auxiliary metadata sets can also be created. These are subsets of metadata that can be attached to objects in the repository. This type of metadata is associated with specific properties of an item, such as image size, the character encoding of a document, or other property that must be tracked for specific items. When creating auxiliary metadata, the database table in which the metadata is stored is also created, with a name given to the table and fields added to it. Note that in order to search for auxiliary metadata, Oracle Text Search (full-text searching) must be used.

The process is the same for creating both types of metadata, either complete auxiliary sets or additional fields with the standard metadata sets. The main difference lies in the creation of the table to store the auxiliary metadata set.

> **Note:**
>
> Using auxiliary metadata sets can slow the search times when using OracleTextSearch because additional tables must be accessed and evaluated.

This section discusses the following topics:

- Creating or Editing Custom Metadata Fields
- Viewing Custom Metadata Field Information
- Deleting a Custom Metadata Field
- Example: Creating a Custom Category Metadata Field

11.7.1 Creating or Editing Custom Metadata Fields

> **Note:**
>
> If you plan to use an option list with the custom field, the option list must be created and populated before creating the custom field.

The following information is a general navigational procedure for adding metadata fields regardless of type (standard metadata or auxiliary metadata).

> **Note:**
>
> Users must have the Records Administrator role or the PCM Administrator role in order to perform this action. The user must also have administrative permissions.

1. Choose **Records** then **Configure**.
2. Choose **Metadata** then **Metadata Sets**.
3. Perform these actions on the Metadata List page:

   To create a **new auxiliary metadata set**, choose **Create Auxiliary Metadata** from the page menu. On the Create or Edit Auxiliary Metadata Set page, enter the auxiliary metadata set name, display name, name of the new table being created to house the metadata set, and column prefix for that table.

   To **add fields to an existing metadata set**, either auxiliary or standard set (Retention Categories, Record Folders, or Physical), choose **Update Fields** from the auxiliary set's individual **Actions** menu on the Metadata List page.
4. On the Create or Edit Standard Metadata Field page, add the field information for the new metadata field.
   - Name: Name for the field in the database. Maximum of 30 characters is allowed. Do not use special characters (question mark, punctuation, and so on).
   - Caption: Caption for the field that will appear in the user interface. Maximum of 30 characters allowed.
   - Type: The data type for the field. Options include:
     - Text (default): Text field, 30 characters maximum.
     - Long Text: Text field, 100 characters maximum.
     - Integer: An integer value ranging from -2^{31} to 2^{31} (-2 billion to +2 billion). Decimal values and commas not permitted.
     - Memo: Text field, 1000 characters maximum.
     - Date: A date field according to the date format specified in system settings. Selecting this type puts the Calendar component icon next to the date field.
   - Default Value: Default value for an option list, Text, or Long Text field. Maximum characters allowed: 30.

- Usage: Select a check box to enable usage. Options include:
  - Required: If selected the column will be required.
  - Enabled: If selected, the field is enabled on pages.
  - Searchable: If selected, the field is added to those fields that are searchable.
- Option List Key: The field used for the option list. Click **Choose** to select a key from a list. Note that an option list must be created and populated before it can be used.
- Option List Type: The kind of option list to use, selectable from a list.

5. Click **Add** (a plus sign) to add the field to the Field list. Click **Delete** (an X) to delete a field from the list. To change the order of fields, highlight a field and move it up or down in the list by clicking the **Up** or **Down** arrow.
6. Click **Apply** after adding or editing all the fields.

11.7.2 Viewing Custom Metadata Field Information

To view information about the custom fields added to metadata sets:

1. Choose **Records** then **Configure**.
2. Choose **Metadata** then **Metadata Sets**.
3. On the Metadata List page, choose **Fields Information** from the **Actions** menu of the metadata set to view.

   The Fields for Metadata page opens showing the specific fields created for that metadata set.

11.7.3 Deleting a Custom Metadata Field

> **Note:**
>
> The Admin.RecordManager right or PCM.Admin.Manager right (when using PCM) is required to perform this action. This right is assigned by default to the Records Administrator and the PCM Administrator roles. The user must also have administrative permissions.

To delete a custom metadata field:

1. Choose **Records** then **Configure**.
2. Choose **Metadata** then **Metadata Sets**.
3. On the Metadata List page, choose **Update Fields** from the set's individual **Actions** menu on the Metadata List page.
4. On the Create or Edit Auxiliary Metadata Set page, select the field name in the Field list and click **Delete** (an X).
5. Click **Apply** after deleting the fields.

11.7.4 Example: Creating a Custom Category Metadata Field

This example creates a custom retention category metadata field that is an optional text box in which you enter an integer value for a SKU (Stock Keeping Unit).

> **Note:**
>
> The Admin.RecordManager right is required to perform this action. This right is assigned by default to the Records Administrator role.

To create a custom retention category metadata field:

1. Choose **Records** then **Configure**.
2. Choose **Metadata** then **Metadata Sets**.
3. On the Metadata List page, choose **Update Fields** in the **Actions** menu for Retention Categories.
4. On the Create or Edit Standard Metadata Field page, complete the metadata fields as follows:
   a. Enter `DeptSKU` as the Name.
   b. In the Type list, select **Integer**.
   c. Enter `Department SKU` as the Caption.
   d. Select **Enabled**.
   e. Select **Searchable**.
5. Click **Add** (the plus symbol).
6. Click **Apply**.
7. To view the new field, browse content and choose **Create Retention Category** from the **Actions** menu.

   The new custom metadata field appears. The Department SKU field is added to the Create Retention Category page.

11.8 Setting Up Workflows

> **Note:**
>
> Workflow creation is only needed to enable category disposition approval processing, reservation processing, or offsite request processing. If you do not need that functionality, you do not need to set up any workflows.

Workflows are used to specify how content is routed for review, approval, and release to the system. A criteria workflow is used for content that enters the review process automatically,

based on metadata matching predefined criteria. A basic workflow is one used to process specific content items.

Three specific criteria workflows must be set up in order for the following functionality to work:

- Category Disposition Approval Processing: Set up to route category dispositions for review and approval.

  If you enable the disposition workflow feature on the Configure Retention Settings page but do not set up the workflow, you must set the `UpdateDispositionsTableOnWorkflowApproval` configuration variable to `false` in the `config.cfg` file.

- Reservation Processing: Set up to route reservation requests for physical content for processing.
- Offsite Processing: Set up to process requests for offsite storage of items.

A workflow is composed of several steps that route the content to groups of people in an alias list. It can be customized to exit when completed, branch content depending on certain conditions, and use variables to designate unknown users. Workflows are discussed in detail in Managing Workflows. This section describes only the information needed to establish the three workflows described previously.

This section discusses the following topics:

- Workflow Prerequisites and Process
- Creating Necessary Workflows

11.8.1 Workflow Prerequisites and Process

The following steps briefly explain the Criteria workflow process and some of the tasks that should be performed before setting up the workflow:

1. A user with Workflow rights sets up the Criteria workflow by defining the following:
   - Security groups: The RecordsGroup, Reservation and Offsite security groups are required.
   - Metadata fields and values: These fields are set up at installation (for example, `OffsiteRequest`.)
   - Review steps and reviewers for each step: It is good practice to discuss workflows with the people involved so they are aware of the responsibilities they will have in the process.
   - If a group of people need to be included in an alias that should be created ahead of time. The following alias lists are needed:
     - Disposition Reviewers: Those people who will review disposition criteria. Suggested name: DispositionReviewGroup.
     - Reservation Reviewers: Those people who can approve reservation requests. Suggested name: ReservationGroup.
     - Offsite Request Reviewers: Those people who review requests for offsite storage. Suggested name: OffSiteRequestReviewGroup.

     See *Administering Oracle WebCenter Content* for details about adding aliases and adding users to alias groups.

2. A user with Workflow rights starts the Criteria workflow by enabling it.
3. When content is checked in with the defined security group and metadata field value, the content enters the workflow.
4. Reviewers for the first step are notified by email that the revision is ready for review.
5. The reviewers approve or reject the revision.
    - If the step is a reviewer/contributor step, the reviewers can check out the revision, edit it, and check it back in before approving it. For example, administrators may need to alter a reservation request.
    - If a user rejects the revision, the workflow returns to the previous contribution step, and the users for that step are notified by email.
    - When the minimum number of users have approved the revision, it goes to next step. If the minimum number of approvals is 0, the revision moves to the next step automatically.
6. When all steps are complete, the revision is released to the system.

11.8.2 Creating Necessary Workflows

This section details the specific requirements for the three workflows needed for the following functionality:

- Category Dispositions Workflow
- Reservation Processing Workflow
- Offsite Storage Workflow

11.8.2.1 Category Dispositions Workflow

The Category Disposition Workflow is used to approve the disposition rules on a category before the rules are enacted.

1. Choose **Administration** then **Admin Applets**.
2. Choose **Workflow Admin** from the Administration Applets list.
3. Click the **Criteria** tab in the Workflow Admin dialog, then click **Add**.
4. Enter the following information in the New Criteria Workflow dialog:
    - Workflow name: `CategoryDispositionsProcess`.
    - Description: `Category Disposition Processing`.
    - Security Group: Select **RecordsGroup** from the list.
    - Original Author Edit Rule: Select **Edit Revision.**
    - Has Criteria Definition: Select this check box.
    - Field: Select **Type** from the list.
    - Operator: This should say Matches.
    - Value: Select **RetentionCategory** from the list.

    Click **OK** when done. The Workflow Admin dialog opens.
5. In the Criteria portion of the dialog, in the Steps section, click **Add**.

6. Enter the following information in the Add New Step dialog:
   - Step name: CategoryDispositionsReview.
   - Description: Review Category Dispositions.
   - Users can review and edit (replace) the current revision: Select this check box.
   - Click the **Users** tab then **Add Alias**. Select the alias list for the users who will review dispositions and click **OK**.
   - Click the **Exit Condition** tab. In the Required Approvers portion, select the check box for **All Reviewers**.
7. Click **OK** then **Enable** in the Workflow Admin dialog to start the workflow.

11.8.2.2 Reservation Processing Workflow

The Reservation workflow is used to process reservation requests for physical items.

1. Choose **Administration** then **Admin Applets**.
2. Choose **Workflow Admin** from the Administration Applets list.
3. Click the **Criteria** tab in the Workflow Admin dialog, then click **Add**.
4. Enter the following information in the New Criteria Workflow dialog:
   - Workflow name: ReservationProcess.
   - Description: Processes reservations.
   - Security Group: select **Reservation**.
   - Original Author Edit Rule: Select **Edit Revision**.
   - Has Criteria Definition: Select this check box.
   - Field: Select **Type**.
   - Operator: This should say Matches.
   - Value: Select **Request**.

   Click **OK** when done.
5. In the Criteria portion of the Workflow Admin dialog, in the Steps section, click **Add**.
6. Enter the following information for the first step in the Add New Step dialog:
   - Step name: RequestReview
   - Description: Review Request
   - Users can review and edit (replace) the current revision: selected.
   - Click the **Users** tab then **Add Alias**. Select the alias list for the users who will review reservation requests and click **OK**.
   - Click the **Exit Condition** tab. In the Required Approvers portion, select **At Least This Many Reviewers** and enter 1 for the value.
   - Click **OK**. The Workflow Admin dialog opens.
7. In the Criteria portion of the dialog, in the Steps section, click **Add**.
8. Enter the following information for the second step in the Add New Step dialog:
   - Step name: RequestComplete

- Description: Complete the request
- Users can review the current revision: selected.
- Click the **Users** tab then **Add Alias**. Select the alias list for the users who will complete the reservation requests and click **OK**.
- Click the **Exit Condition** tab. In the Required Approvers portion, select **At Least This Many Reviewers** and enter 0 for the value.
- Click the **Events** tab.
  - Click **Edit** in the Entry section. Click the **Custom** tab then select **Custom Script Evaluation**. Enter the following code

    ```
    <$wfSet("wfJumpName", "complete")$>
        <$wfSet("wfJumpEntryNotifyOff", "1")$>
    ```

    Click **OK**.
  - Click **Edit** in the Update section. Click the **Custom** tab then select **Custom Script Evaluation**. Enter the following code:

    ```
    <$if parseDate(dOutDate) < parseDate(dateCurrent(1))$>
        <$wfSet("wfJumpName", "complete_update")$>
        <$wfSet("wfJumpTargetStep", wfCurrentStep(10))$>
        <$wfSet("wfJumpEntryNotifyOff", "1")$>
    <$endif$>
    ```

    Click **OK**.

9. Click **OK** then **Enable** in the Workflow Admin dialog to start the workflow.

11.8.2.3 Offsite Storage Workflow

The Offsite Storage workflow is used to process requests to store physical items offsite.

1. Choose **Administration** then **Admin Applets**.
2. Choose **Workflow Admin** from the Administration Applets list.
3. Click the **Criteria** tab in the Workflow Admin dialog, then click **Add**.
4. Enter the following information in the New Criteria Workflow dialog:
   - Workflow name: OffsiteProcess.
   - Description: Processes Offsite Requests.
   - Security Group: select **Offsite**.
   - Original Author Edit Rule: select **Edit Revision**.
   - Has Criteria Definition: selected.
   - Field: select **Type**.
   - Operator: this should say Matches.
   - Value: select **Offsiterequest**.

   Click **OK** when done. The Workflow Admin dialog is opens.
5. In the Criteria portion of the dialog, in the Steps section, click **Add**.
6. Enter the following information for the first step in the Add New Step dialog:
   - Step name: OffsiteRequestReview.

- Description: Review Offsite Request.
- **Users can review and edit (replace) the current revision**: selected.
- Click the **Users** tab then **Add Alias**. Select the alias list for the users who will review reservation requests and click **OK**.
- Click the **Exit Condition** tab. In the Required Approvers portion, select **At Least This Many Reviewers** and enter 1 for the value.

7. Click **OK** then click **Enable** in the Workflow Admin dialog to start the workflow.

11.9 Configuration with Desktop Integration Suite

When using Oracle DIS with the Records system with the DoD compliance component enabled, users may not be able to check in files by copying and pasting or by dragging and dropping them into contribution folders. DoD compliance requires that the Category or Folder fields be required during checkin, that means an item cannot be checked in if the field is empty.

Because copying and pasting or dragging and dropping into a folder often does not require any additional user interaction, the check-in will not complete successfully unless the administrator configures the Records system to enable such checkins.

Several workarounds for this issue are available:

- Set default metadata for the folders by selecting the category and folder from the available selections
- Set default metadata for users by creating a global rule when setting up profiles.
- Change the configuration of the system by setting the `dodSkipCatFolderRequirement` variable.

11.10 Configuration Variables

Several configuration variables can be included in a configuration file to change the behavior or interface of the software. In addition to the configuration variables described here, flags in the `rma_email_environment.cfg` file can be set to determine which fields can be edited during events such as check-in and update for e-mail content. The flags are a double-colon-separated list.

The following is an overview of the more commonly used configuration variables. For details about each variable, see *Configuration Reference for Oracle WebCenter Content*.

- `AllowRetentionPeriodWithoutCutoff`: Used to specify retention periods for triggers.
- `dodSkipCatFolderRequirement`: Allows items to be checked in without specifying a category or folder for the checkin. If a DoD configuration is in use, this causes non-conformance with DoD regulations.
- `HideVitalReview`: Used to hide the Subject to Review fields.
- `RecordsManagementDenyAUthorFreePassOnRMSecurity`: Allows the author of content to delete content they authored regardless of the user's security settings.
- `RecordsManagementNumberOverwriteOnDelete`: Sets the number of disk scrubbing passes used for a destroy action.

- `RmaAddDocWhereClauseForScreening`: Allows users with the Records Administrator role to screen for frozen items to which they do not have access (using ACLs) on the screening page or on the Freeze Information page.
- `RmaAllowKeepOrDestroyMetadataOption`: Allows the option to keep or destroy metadata when using the following disposition actions: Delete All Revisions, Accession, Archive, Move, and Transfer.
- `RmaEnableWebdavPropPatchOnExport`: Enables WebDAV support of a PropPatch method to assign metadata values to a file that has been uploaded to a WebDAV server.
- `RmaEnableFilePlan`: Enables the File Plan folder structure.
- `RmaEnableFixedClone`: Enables the fixed clone functionality that allows the creation of record clones of content revisions.
- `RmaEnablePostFilterOnScreening`: Enables additional security on screening results. If a user does not have appropriate security for an item in a screening result list, that item is hidden from view.
- `RmaFilePlanVolumePrefix` and `RmaFilePlanVolumeSuffix`: Defines the naming convention for volumes.
- `RmaFixedClonesTitleSuffix`: Used to set the suffix that is automatically appended to a fixed clone content item.
- `RMAHideExternalFieldsFromSearchInfo` and `RMAHideExternalFieldsFromCheckInUpdate`: Used to hide external fields on the noted pages. The default setting is TRUE, so External fields are hidden on those pages.
- `RmaNotifyDispReviewerAndCatAuthor`: Used to control who is notified about disposition actions.
- `RmaNotifyReviewerAndAlternateReviewer`: Used to control what reviewers are notified about actions.
- `sceUseNativeInDataFeeds`: Used to control whether the SES search will pick up the web viewable file or the native file.
- `ShowContentForStorageBrowse`: Used to show content items in the storage browse pages.
- `SimpleProfilesEnabled`: Used to enable Simple Profile functionality.
- `UieHideSearchcheckboxes`: Used to show or hide the metadata field check boxes on the search page, which limit the number of metadata fields initially shown on the page.

12

Managing a Records Retention Schedule

A retention schedule is an organized hierarchy of series, categories, and record folders that can cluster content into similar groups, each with its own retention and disposition characteristics. This chapter discusses how to set up a retention schedule and how to process retention assignments.
This chapter discusses the following topics:

- Understanding Retention Schedules
- Using a Series
- Managing Retention Categories
- Managing Record Folders

12.1 Understanding Retention Schedules

> **Note:**
>
> If a retention schedule contains 10,000 or more series, categories, and folders, then the database administrator should build database indexes on the tables to enhance performance. For record folders, add indexes on the columns of the Folders table. For retention categories, add indexes on the columns of the Categories and Dispositions tables. For series, add indexes on the columns of the Series table. For further information about defining an index on a table column, see the database documentation.

Many different retention schedules can be created for the requirements mandated by an organization.

If the RoleEntityACL component is enabled in Content Server, that component does not affect any retention objects such as categories or folders. Therefore, the ability to use ACLs on a URM role is not enabled on category creation pages or folder creation pages even if the RoleEntityACL component is enabled. The use of role ACLs is enabled on the check-in page if the component is enabled.

> **Note:**
>
> The retention schedule is not a contribution mechanism, but rather a disposition mechanism. It defines how and when content should be processed during its life cycle. It is not intended to check content into the repository.

This section discusses the following topics:

- Retention Schedules and MoReq2 File Plans

- Retention Schedules and Folders Retention Functionality
- Planning a Retention Schedule
- Creating and Navigating Object Levels

12.1.1 Retention Schedules and MoReq2 File Plans

To enable MoReq2 file plans, set the `RmaEnableFilePlan` configuration variable to TRUE and restart Content Server. The file plan is used by selecting **Browse Content**.

A file plan has a strict folder hierarchy consisting of four node types: Class, File, Sub-File and Volume, with only Classes allowed at the top level of the hierarchy. Classes provide a framework for classification and files are used to store like records.

Files and Classes cannot be mixed at a single node in the hierarchy. For example, if a Sub-File is placed in a File folder, that File folder cannot contain any other type of item, including content. The exception is if a folder type contains content items, it can also contain volumes. Classes can contain other Classes, Files, or content. Sub-files can contain content items. Volumes can only contain content. The Records software has been configured to allow Create access only to those items that are allowed at the specific point in the hierarchy.

For more details about file plan nodes and the hierarchy, see *Model Requirements for the Management of Electronic Records*.

Functionality for using the file plan is similar to that for the retention schedule. One major difference is that disposition actions are applied to Classes by linking the class to a category that has a disposition schedule.

When reviewing the information in this chapter, consider how the information can apply to a file plan as well as any retention schedule.

12.1.2 Retention Schedules and Folders Retention Functionality

Folders Retention functionality is not available if DoD Baseline or DoD Classified is enabled.

The Folders Retention functionality is enabled when the FrameworkFolders component is enabled. Folders Retention allows you to group content items in a retention query folder then apply a retention action to the content in the folder. It does not apply the retention action to the folder itself.

If a content item has dispositions defined in both Content Server and in the Records system, only the disposition and schedule defined by the Records system is used.

> **Note:**
>
> Because the life cycle information is not viewable when using Retention Folders, it is recommended that you use this functionality for less important items that do not need to be retained or tracked, such as drafts of documents or temporary items. More important documents that need to be tracked and retained should be handled using the Records retention schedules.

Retention actions include the following:

- Retention By Revision: used to specify how many revisions of an item to keep. For example, if a content item in the query folder has 8 revisions, when the retention rule is run, the first 3 revisions are deleted and the latest 5 revisions are retained. If the Records system is installed, an item will not be deleted if it is frozen.
- Retention By Age: used to specify how long an item exists before it is deleted. If the Records system is installed, the options for periods are the periods specified in the Records configuration. If the Records system is not installed, all default periods except for fiscal periods are included.
- Retention By Category (only available if the Records system is installed and enabled): used to specify a category disposition to apply to a query folder. This is similar to specifying a category ID on a content item.

  When specifying this option, you can also specify if the action requires approval. Approval is performed in the same manner as approvals in the Records system.

The following list summarizes the actions available with Retention Folders:

- If Records *is not* enabled:
  - Retention By Category is not available for use
  - Retention By Revision AND Retention By Age can be combined
- If Records is enabled:
  - Retention By Category is available for use

Delete dispositions in Folders Retention are treated differently than deletions in the Records system. The shortest delete interval is used in Folders Retention instead of the longest interval as is used in Records.

Folders Retention differs from using a Records retention schedule in that the life cycle of content managed by Folders Retention is not visible to the user. When content is managed through the Records system, the life cycle of the disposition schedule is displayed by browsing for the folder then clicking **Information** then **Life Cycle** from the folder's **Actions** menu.

Folders Retention functionality can only be set up and managed by users with Content Server administrative privileges. A user with Records Administrator privileges cannot set up Folders Retention functionality unless that user also has Content Server administrative privileges.

For details about accessing and setting up the Folders Retention functionality, see Managing Folders.

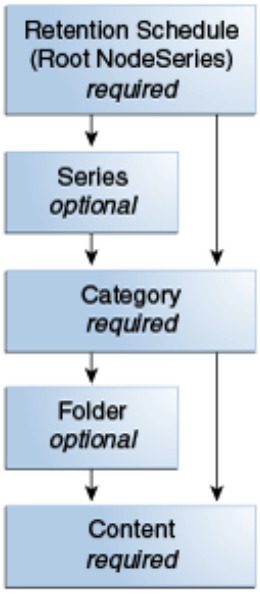
12.1.3 Planning a Retention Schedule

Do not base a category on a dynamic feature such as organization hierarchy because organizations are reorganized on a frequent basis. Use static divisions for category departments, and be more generic with categories. Record folders can be more specific.

12.1.3.1 Retention Schedule Hierarchy

A typical hierarchy of a retention schedule consists of series, categories, and/or record folders. Series are optional top-level nodes that can be nested. A retention category cannot be nested, due to the nature of its disposition schedules. Record folders can be nested. Figure 12-1 shows the basic hierarchy of retention schedule objects.

Figure 12-1 Basic Retention Schedule Hierarchy



Content is filed directly into a retention category, and optionally can be filed into a record folder under a retention category. The retention schedule is the top-most series root node. The top node is created automatically.

The remaining retention schedule objects (series, folder, or retention category) are created by the Records Administrator. Users or administrators create content for filing within the application. A series is an optional container created by the Records Administrator. A retention category is required, and it contains disposition instructions for processing content. A record folder is optional, and it also organizes content according to some commonality.

Figure 12-2 shows the main characteristics of each retention schedule object at a glance. Series do not have security set directly on the series object, whereas retention categories, record folders, and content all have a variety of security options, including Access Control Lists (ACLs), supplemental markings, custom security fields, and (custom) classifications.

Figure 12-2 Attributes of Retention Schedule Objects

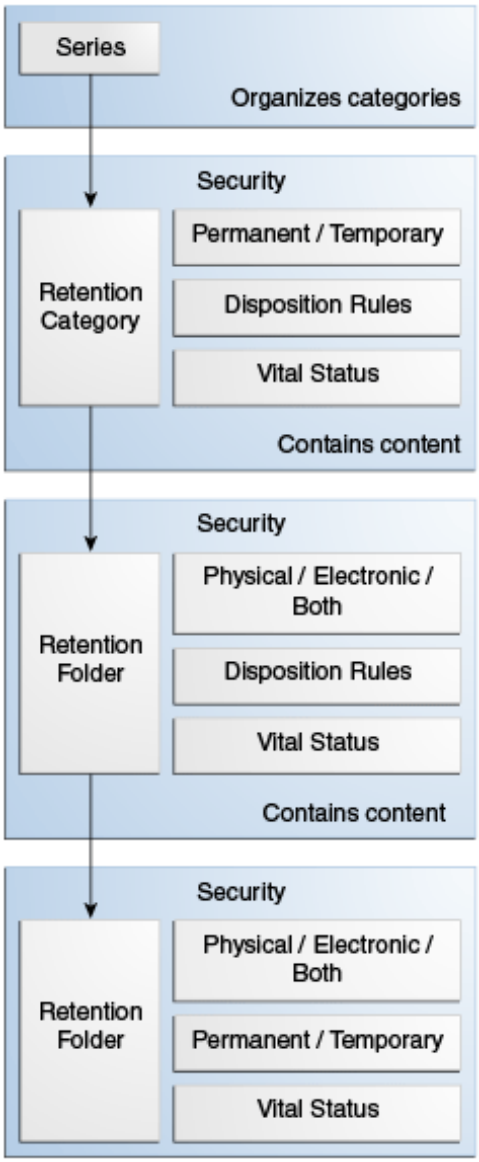
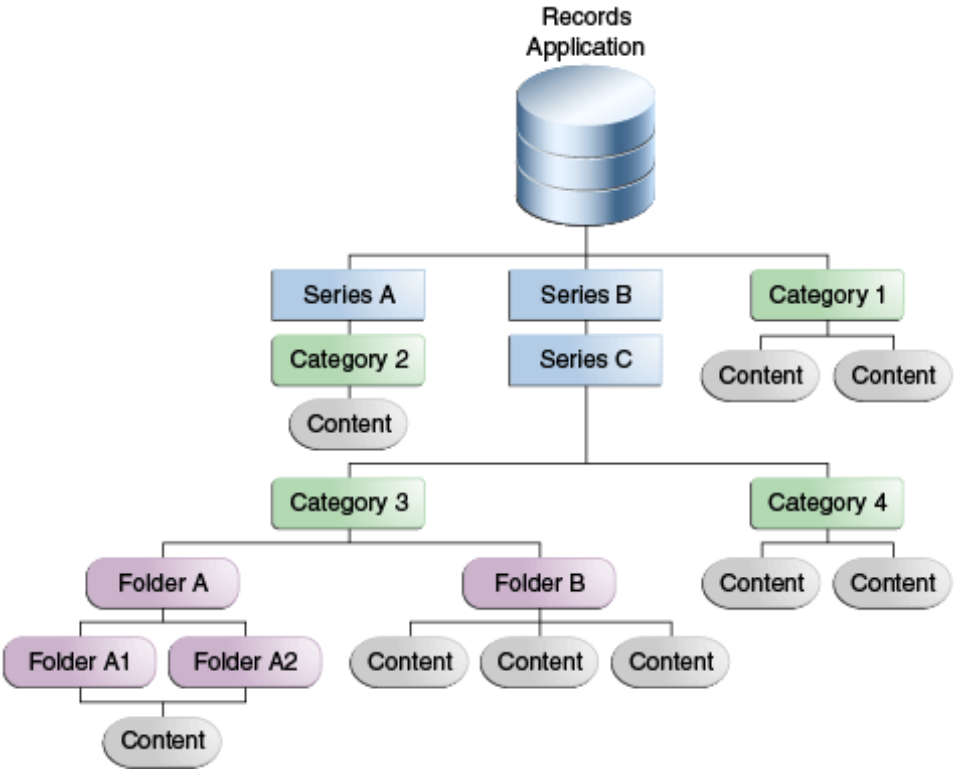


Figure 12-3 illustrates a slightly more complex retention schedule hierarchy, with:

- Nested series (Series B and C).
- Nested folders (Folders a1 and a2 under Folder a).
- Content filed directly into a category (Categories 1, 2, and 4) rather than a folder.
- Categories without a series (Category 1).
- An item filed into multiple folders (Folders a1 and a2).

Figure 12-3 Sample Retention Schedule Hierarchy



While it is possible to file content into multiple locations in the retention schedule, this is not recommended due to the complexity of processing multiple disposition schedules. For best performance results, content should be filed into a single folder or category. When multiple disposition schedules are attached to an item, the item is processed by the disposition with the longest retention period.

12.1.3.2 Retention Schedule Attributes

Some of the attributes of retention schedule objects are inherited from parent objects. In certain cases, the attributes can be overridden at a lower level.

Review status, which includes the review period and reviewer, can be set at the retention category level, folder level and the item level. The lowest level (the item level) takes precedence if all information is of equal duration and is set at the category, folder, and item levels.

In the case of review periods with differing lengths between a parent and child objects, the shortest review period takes precedence for a child folder and is indicated in the relevant content information pages. The longer review period is ignored. If the shorter review period is removed or changed, the longer review period is used again in cycling reviews for content.

> **Note:**
>
> Within a parent and child object hierarchy, the review period with the shortest review period takes precedence for a child folder over a longer review period set on the child folder.

For example, a subject-to-review category has a review period of two calendar quarters. A child folder within the subject-to-review category has a review period set as four calendar quarters. Because the category higher in the hierarchy (the parent) has a shorter review period, the child folder ignores its own longer review period setting. In essence, the folder has a review period override in effect.

If the review status is not set at the record folder level for a record folder in a subject-to-review category, the folder *always* inherits review status from the category. At the content level, a content can inherit review information from the category, and the content can inherit information from the folder if it does not have its own review settings.

If a content item is filed directly into a subject-to-review retention category, it inherits settings from the category. If a subject-to-review item is filed into a subject-to-review record folder, it inherits settings from the immediate parent folder. Because record folders can be nested, the immediate folder parent determines review attributes for the item.

If a retention category is subject to review, and none of the folders or content items have their own review settings, then the folders and the items all inherit review attributes from the category.

You can create a non-review retention category containing record folders, content, and items subject to review. The reverse is not possible. You cannot create a retention category that is subject to review containing non-subject-to-review record folders and items due to inheritance of the subject to review attributes.

Permanent items cannot be destroyed by a disposition instruction. Permanent items typically are a small percentage of an organization's information base. Permanent status is determined by the National Archives and Records Administration (NARA) as having sufficient historical value to warrant continued preservation beyond the normal time needed for administrative, legal, or fiscal purposes. Permanent items are sometimes referred to as **archival** items.

12.1.3.3 Disposition Instructions

Disposition instructions are defined at the retention category level, with some rules being applied uniquely to a child record folder. A record folder inherits disposition rules from the retention category. Content items inherit dispositions from their retention category, and if applicable, a folder with its own uniquely applied disposition rule. For more information, see Defining and Processing Dispositions.

12.1.3.4 Frozen Folder and Content Status

Freezing a record folder inhibits disposition processing for the folder and its child folders and content.

Record folders and content items inherit the freeze status if it is present on an ancestor. In addition to inheriting the freeze status, freezes can be performed at lower levels within a

hierarchy where inheritance is not present. A child record folder or an item within a record folder can be frozen.

Freezing a content item outside of a folder also inhibits disposition processing and prevents the metadata was being updated.

12.1.4 Creating and Navigating Object Levels

To use any retention objects, choose **Browse Content**. Depending on a user's rights and role, the user can browse all Retention Schedules or just the ones created by that user.

A user must be at a certain context, or level, within the retention schedule to work with retention schedule objects. Depending on the location within the hierarchy, different menu options appear in the main **Actions** menu when browsing the retention schedule.

The following table shows what retention schedule objects can be created at each level.

At this level:	You can create:
Series or root node	• Series • Retention category
Retention category	• Record folder • Content item
Record folder	• Record folder • Content item

The main root node is considered the retention schedule series node. At the series level, a series or retention category can be created.

Menus are relative to the location in the hierarchy. For example, at the Folder level you can create a folder or content. You cannot create a category.

The following list describes the possible menu options that may appear depending on the location in the hierarchy. These options may appear on an individual item's **Actions** menu or on the page menu.

Information in parenthesis indicates the area of the hierarchy where the information appears.

- Information
  - Category Information (Category level): Opens the Retention Category Information page.
  - Series Information (Series level): Opens the Series Information page.
  - Folder Information (Folder level): Opens the Record Folder Information page.
  - Metadata History (Category level and Folder level): Opens the Metadata History page.
  - Disposition Information (Category level): Opens the Disposition Information page.
  - Life Cycle (Folder level): Opens Life Cycle information.
  - Recent Reviews (Folder level): Opens review history information.

  - Retention Schedule Report (all): Creates a retention schedule report in the format specified when the system was configured.

- Edit
  - Edit Retention Category (Category level): Opens the Create or Edit Retention Category page.
  - Edit Disposition (Category level): Opens the Disposition Instructions page.
  - Edit Review (Category level and Folder level): Opens the Edit Review information page.
  - Edit Series (Series level): Opens the Create or Edit Series page.
  - Move (all): Opens the Select Retention Series, Record Folder or Category dialog.
  - Hide (Series level): Opens a prompt to indicate why the object is being hidden.
  - Freeze/Unfreeze (Folder level): Toggles between freeze or unfreeze for a record folder.
- Copy: Copies the object in question.
- Delete: Deletes any checked objects. If an object has content (for example, a folder) an error message is displayed and the object is not deleted.
- Create
  - Create Record Folder (Category level and Folder level): Opens the Create or Edit Record Folder page.
  - Check In Content (Category level and Folder level): Opens the Content Checkin page.
  - Check in Physical Item: Opens the Create Physical Item page.
  - Create Series (Series level): Opens the Create or Edit Series page.
  - Create Retention Category (Series level): Opens the Create or Edit Retention Category page.
- Change View
- – Thumbnail: Presents a icon-based view.
  - Headline: Presents a horizontal, textual view.

In addition, the following options may be available on the individual item's **Actions** menus on the Folder page and on the table menu on the Folder level:

- Set Dates
  - Mark reviewed: Marks a folder as reviewed.
  - Mark recursive: Marks all child objects as reviewed.
  - Cancel: Marks the folder as canceled, making it obsolete.
  - Expire: Expires all objects in a folder.
  - Obsolete: Marks content and the folder as obsolete. This toggles to Undo Obsolete if a folder becomes obsolete due to specific actions.
  - Rescind: Rescinds a folder and the items therein.
  - Undo Cutoff (table menu only): Reverses the cutoff status of a folder.

  - Undo Obsolete (table menu only): Marks items and the folder as not obsolete. To undo the obsolete status for content items, you must search for the items, select the check boxes for those items to be marked, then select **Clear Dates** then **Obsolete** from the **Set Dates** menu.
- Add to Favorites: Used to add the marked object to the Favorites list.

12.2 Using a Series

> **Note:**
>
> The appropriate rights are required to work with series. There are separate rights for reading (viewing), creating, deleting, moving, editing, and hiding/unhiding series. The predefined Records User and Records Officer roles can only read (view) series. The predefined Records Administrator role can perform any of the other series-related tasks.

A series is an optional feature for organizing content. If an organization has a multitude of retention categories, setting up series can assist with managing the view of the retention schedule hierarchies. Series should be a static and non-specific method of organization: for example, `Buildings` not `7500 Building`. This allows the hierarchy to remain static over time. Series can be nested within each other.

Series are also useful for creating work-in-progress retention schedules because series can be hidden from users, which prevents people from filing any data into the hidden series.

The following tasks are involved in managing series:

- Creating or Editing a Series
- Viewing Series Information
- Hiding and Unhiding a Series
- Moving a Series
- Deleting a Series

The retention schedule can be accessed in two ways:

- Choose **Browse Content** then **Retention Schedule**.
- Choose **Records** then **Retention Schedules**.

12.2.1 Creating or Editing a Series

> **Note:**
>
> The Series.Create right is required to perform this action. This right is assigned by default to the Records Administrator role.

Nested series (a series within a series) is allowed. To create a series:

1. Access the retention schedule and navigate to the location in which to create the series.
2. Choose **Create** then **Create Series** from the **Actions** menu in an existing series or from the page menu.
3. On the Create or Edit Series page, enter an identifier for the series.
4. Enter a name for the series.
5. Click **Create**.

   The series is shown in both the Browse Content area and in the Retention Schedule list.

> **Note:**
>
> The Series.Edit right is required to perform this action. This right is assigned by default to the Records Administrator role.

To edit a series:

1. Access the retention schedule. Choose **Edit** then **Edit Series** in the **Actions** menu for the series to edit.
2. On the Create or Edit Series page, enter any changes to the value in the Series Name box.
3. Click **Submit Update**.

   A message appears saying the series was updated successfully.
4. Click **OK**.

12.2.2 Viewing Series Information

> **Note:**
>
> The Series.Read right is required to perform this action. This right is assigned by default to the Records Administrator role.

To view information about a series:

1. Access the retention schedule. Click the **Info** icon for the series to view.

   The Series Information page opens. This page shows relevant information about the selected series.
2. Click **OK** when done.

12.2.3 Hiding and Unhiding a Series

> **Note:**
>
> The Series.Hide/Unhide right is required to perform these actions. This right is assigned by default to the Records Administrator role.

A hidden series and its children are not visible to anyone without the Series.Hide/Unhide right. This feature provides a staging area for setting up and testing retention schedules. After a retention schedule is ready for production, unhide the series.

To hide a series:

1. Access the retention schedule. Choose **Edit** then **Hide Series** from the **Actions** menu for the series to hide.
2. Enter a reason (optional) and click **OK** to confirm or leave the text box empty. Click **Cancel** to abort the entire action.

   If confirmed, the series icon is now semi-transparent to indicate it is hidden.

Follow the same procedure to unhide the series. Access the retention schedule then choose **Unhide Series** in the item's **Actions** menu. If the action is confirmed, the series icon is no longer semi-transparent to indicate it is not hidden.

12.2.4 Moving a Series

> **Note:**
>
> The Series.Move right is required to perform this action. This right is assigned by default to the Records Administrator role.

All child series, categories, record folders and content items move with the parent series.

To move a series:

1. Access the retention schedule. Choose **Edit** then **Move Series** from the **Actions** menu for the item to move. To move multiple items, select the check box for the series and choose **Move** from the table menu.
2. In the Select Retention Series, Record Folder or Category dialog, click to expand the tree, and click the series that will contain the item.

   The location field populates with the new location.
3. Click **OK**.

   The Exploring Series page shows the series in its new location.

12.2.5 Deleting a Series

> **Note:**
>
> The Series.Delete right is required to perform this action. This right is assigned by default to the Records Administrator role.

If a series is populated a message appears when an attempt is made to delete the series, prompting the user to delete the contents as well as the series. Be sure to move any content, record folders, categories, and any nested series from the series to be deleted if any of those objects should be retained.

To delete a series:

> **Tip:**
>
> To delete multiple items, select the check box for the items and choose **Delete** from the table menu.

1. Access the retention schedule. Choose **Delete** then **Delete Series** from the **Actions** menu for the item to delete.
2. You are prompted to confirm the deletion. Click **OK** to delete the series, or **Cancel** to cancel the delete action. To delete any child objects, select the check box for **Include child content items** on the prompt that appears. Click **Yes** when done.
3. Enter a reason and click **OK** to confirm or leave the text box empty and click **OK**. Click **Cancel** to abort the entire action.

   If confirmed, the series is deleted from the retention schedule.

12.3 Managing Retention Categories

> **Note:**
>
> The appropriate rights are required to work with categories. There are separate rights for reading (viewing), creating, deleting, moving, and editing categories. The predefined Records User and Records Officer roles can only read (view) categories. The predefined Records Administrator role can perform any of the other category-related tasks.

A retention category is a retention schedule object with associated security settings and disposition instructions defined. Retention categories cannot be nested within other retention categories because they are disposition instructions, not an organization container. They are a method of grouping content with the same disposition requirements.

When retention categories are sorted and listed, they are listed on a per-source basis. For example, if three sources are used (Source1, Source2, Source3), all items from Source1 are sorted as a separate group, items from Source2 are sorted as a separate group, and items from Source3 are sorted as a separate group. Then items from each source are displayed in a round-robin style with the first item of Source1, the first item from Source2, and the first item from Source3, followed by the second item of each source.

If ACLs are on the retention category, the user must also be on the ACL to view or access the retention category. At the category level, record folders or content items can be created.

The following tasks are involved in managing retention categories:

- Creating or Editing a Retention Category
- Viewing Retention Category Information
- Viewing Category Metadata History
- Copying a Retention Category
- Moving a Retention Category
- Deleting a Retention Category
- Retention Category Example

The retention schedule can be accessed in two ways:

- Choose **Browse Content** then **Retention Schedule**.
- Choose **Records** then **Retention Schedules**.

12.3.1 Creating or Editing a Retention Category

> **Note:**
>
> The Category.Create right is required to perform this action. This right is assigned by default to the Records Administrator role.

Retention categories can be created at the root node level or within a series.

12.3.1.1 Creating a Retention Category

To create a category:

1. Choose **Browse Content** then **Retention Schedules**.
2. Choose **Create** then **Create Retention Category** from the table menu.
3. On the Create or Edit Retention Category page, accept the default security group or select a group from the **Security Group** list. The **Default Content Server security** check box must be selected on the Configure Retention Settings page.
4. (Optional) If Accounts are enabled, choose the associated account for the category.

5. (Optional) If default security is used on categories, select an author of the retention category from the **Author** list. The author defaults to the user currently logged in and entering the information.
6. Enter a unique identifier for the category.
7. Enter a name for the category.
8. Enter a description with a maximum of 1000 characters.
9. (Required for U.S. Government Agencies) Enter the code of the authority for the disposition in the **Disposition Authority** box. Private sector organizations can enter the person or department responsible for the category, or enter *none*.
10. To restrict revisions of items in the category, select **Restrict Revisions**.
11. To restrict deletions of items in the category, select **Restrict Deletes**.
12. To restrict edits of items in the category, select **Restrict Edits**.
13. If the retention category is to contain content for review, and all objects should inherit the subject to review status, do the following:
    a. Select **Subject to Review**.
    b. To specify a reviewer for the retention category rather than allow the reviewer to revert to the notify recipient system default, select a reviewer from the **Reviewer** list. When selecting a reviewer, make certain that user has the rights required to perform the review. Otherwise an error message is displayed and the user cannot perform the review.
    c. Enter an integer value for the number of review periods.
    d. Select the defined period from the **Review Period** list.
14. (Optional) If Access Control Lists (ACLs) are used, assign group permissions to the category:
    a. To assign group permissions, click **Select** near **Group Permissions**.
    b. On the Select Alias page, select or type the alias, enable the Read, Write, Delete, and Admin permissions as appropriate for the alias, and click **Add to List**. Repeat this step for each alias for which to set permissions, and click **OK**. The alias and its permissions show in the Group Permissions text box of the Create Retention Category page.
15. (Optional) If Access Control Lists (ACLs) are used, assign user permissions to the category:
    a. Click **Select** next to the **User Permissions** box.
    b. On the Select User page, select or type the user, enable the Read, Write, Delete, and Admin permissions as appropriate for the user, and click **Add to List**. Repeat this step for each user for whom to set permissions, and click **OK**. The user and their permissions show in the User Permissions text box of the Create Retention Category page.
16. Click **Create**.

    The Dispositions Instructions page opens. Create a disposition rule or click **Submit Update** to create a rule later.

> **Note:**
>
> The Category.Edit right is required to perform this action. This right is assigned by default to the Records Administrator role.

12.3.1.2 Editing a Retention Category

To edit an existing retention category.

1. Access the retention schedule. Choose **Edit** then **Edit Retention Category** from the item's **Actions** menu.
2. On the Create or Edit Retention Category page, enter changes to the available fields.
3. Click **Submit Update**.

   The successfully updated retention category message appears.
4. Click **OK**.

   The Exploring Retention Schedule page opens.

12.3.2 Viewing Retention Category Information

> **Note:**
>
> The Category.Read right is required to perform this action. This right is assigned by default to the Records Administrator role.

1. Access the retention schedule. Click the **Info** icon for the item to view.

   The Retention Category Information page opens. This page shows relevant information about the selected retention category.
2. Click **OK** when done.

12.3.3 Viewing Category Metadata History

> **Note:**
>
> The Category.Edit right is required to perform this action. This right is assigned by default to the Records Administrator role.

The metadata history of a retention category shows a list of all changes made to the editable category properties.

To view metadata history:

1. Access the retention schedule. Choose **Information** then **Metadata History** from the item's **Actions** menu.
2. The Metadata History page opens, showing a list of all changes made to the editable category properties. The following information is provided:
   - The user who made the change.
   - The timestamp when the change was made.
   - The affected field(s).
   - The old and new field values.
3. Click **OK** when done.

12.3.4 Copying a Retention Category

> **Note:**
>
> The Category.Copy right is required to perform this action. This right is assigned by default to the Records Administrator role.

To copy a retention category:

1. Access the retention schedule. Find the category to copy and choose **Copy** from the item's **Actions** menu.
2. The Create or Edit Retention Category page opens with some fields already filled in. Edit the remainder of the fields as needed.
3. Click **Submit Update**.

   The Dispositions Instructions page opens. Create a disposition rule or **Submit Update** to create a rule later.

12.3.5 Moving a Retention Category

> **Note:**
>
> The Category.Move right is required to perform this action. This right is assigned by default to the Records Administrator role.

A retention category can be moved to another series or to the root node retention schedule level. To move a category:

1. Access the retention schedule. Choose **Edit** then **Move** from the item's **Actions** menu.
2. On the Select Retention Series, Record Folder or Category dialog, click to expand the tree, and click the series to which to move the category. The location field populates with the new location.
3. Click **OK**.

The Exploring Series page and Browse Content area show the retention category in its new location.

12.3.6 Deleting a Retention Category

> **Note:**
>
> The Category.Delete right is required to perform this action. This right is assigned by default to the Records Administrator role. Delete permission (D) for the RecordsGroup security group is also required.

To delete a retention category:

1. Access the retention schedule. Choose **Delete** then **Delete Category** from the item's **Actions** menu.
2. You are prompted to confirm the delete. Click **OK** to delete the category, or **Cancel** to cancel the delete. To delete any child objects, select the check box for **Include child content items** on the prompt that appears. Click **Yes** when done.
3. You are prompted to enter a reason for the action. Enter a reason and click **OK** to confirm or leave the text box empty, and click **OK**. Click **Cancel** to abort the entire action.

   If confirmed, the retention category is deleted from the retention schedule.

12.3.7 Retention Category Example

This example creates an archive disposition action for the retention category to be reviewed. This example retention category has a three month review period.

1. Choose **Browse Content** then **Retention Schedules**.
2. On the Exploring Retention Schedule page, choose **Create** then **Create Retention Category** from the table menu.
3. On the Create or Edit Retention Category page, enter **`RCV-101`** for the Retention Category Identifier.
4. Enter **`Operational for Review`** for the Retention Category Name.
5. Enter **`RCV-101`** for the Retention Category Description.
6. (Required for U.S. Government Agencies) Enter **`RCV-101`** as the code of the authority for the Disposition Authority.
7. Select **Subject to Review**.
8. Specify a Reviewer and a Review Period.
9. Click **Create**. Perform the following actions on the Disposition Instructions page:
   a. Click **Add**.

      The Disposition Rule page opens.

   b. Select **Retention Period Cutoff** for the **After** field (alternate label: Triggering Event).

c. Enter **`3 Calendar Months`** in the **Wait For** field (alternate label: Retention Period).

d. Select **Notify Authors** from the **Do** list (alternate label: Disposition Action).

e. Click **OK**.

10. Click **Submit Update**.

11. Click **OK**.

12.4 Managing Record Folders

Retained items differ from other documents in the repository because they have different metadata are associated with a disposition life cycle. A record folder organizes similar items within a retention category. A retention category can have multiple record folders, and record folders can be nested within other record folders.

If a record folder does not have its own security settings, the folder inherits security settings from its parent retention category. Each record folder can have its own security settings that further limit access to the items in that folder. Record folders can be further secured by using supplemental markings and custom security fields.

Record folders for temporary content are destroyed with temporary content as part of final disposition processing. Records administrators create new record folders as necessary to accommodate processing temporary items. Record folders for content subject to review and permanent content are not destroyed, and do not have to be re-created due to final disposition.

Record folders can inherit disposition rules from their parent record folder or category. Separate disposition instructions for individual folders can be set up as well. This is done when the dispositions are created for the category where the folder is stored. It is not done during the creation of the folder.

In addition to inheriting security settings and disposition rules, folders also inherit content review information from the parent category. If a folder is inheriting review information, it is indicated on the Record Folder Information page. The review information taking precedence is at the lowest node (the shortest review period prevails), such as in the case of nested folders. Review information can be overridden at the folder level. For example, you can specify a different reviewer or review period cycle but you cannot specify a folder within a subject-to-review retention category as a folder that is not subject to review. If you do not want a record folder to be reviewed, you must create the folder in a non-subject-to-review category.

It may be necessary at times to create a volume for a folder. When a volume is created, the content in that folder is moved to the newly created *volume folder*. The folder uses a naming convention of *prefix*+timestamp+*suffix*. Both *prefix* and *suffix* can be defined by setting configuration variables. For details, see *Configuration Reference for Oracle WebCenter Content*. If neither is defined, a prefix of `volume_` is used.

After the volume is created and the content placed inside, the folder is closed and cut off. Subsequent content items can be checked in to the parent folder and additional volumes can be created. The Cutoff and Create Volume disposition action do this. Volumes are used in retention schedules as well as file plans (used for MoReq tracking).

> **Note:**
>
> The appropriate management rights to work with record folders are required. Separate rights are required for reading (viewing), creating, deleting, opening/closing, editing, moving, and freezing/unfreezing folders. The predefined Records User role can only read (view) record folders. The predefined Records Officer role can read, create, edit, and move folders. The predefined Records Administrator role can perform all folder-related tasks.

This section discusses the following topics:

- Creating a Record Folder
- Creating a Volume Folder
- Editing a Record Folder
- Changing the Disposition Applied to a Folder
- Moving a Record Folder
- Closing or Unclosing (Reopening) a Record Folder
- Freezing or Unfreezing a Record Folder
- Canceling_ Expiring_ and Rescinding Folders
- Deleting a Record Folder
- Setting Dates with External Folders
- Classification Settings for Folders
- Folder Examples

12.4.1 Creating a Record Folder

> **Note:**
>
> The Folder.Create right is required to perform this action. This right is assigned by default to the Records Officer and Records Administrator roles.

To create a record folder within a retention category, or as a child folder of another record folder:

Prerequisites

- Create a retention category
- Configure the time periods (for cycling items for review).
- Create a Supplemental Marking (optional)

This procedure also assumes that security is configured and rights are assigned to users.

1. Open the retention category or folder in which to create a folder.

2. Choose **Create** then click **Create Records Folder** from the page **Actions** menu.
3. On the Create or Edit Record Folder page, accept the RecordsGroup as your default security group or select a different group from the Security Group list.
4. (Optional) If your organization uses accounts in its security model, select the account associated to the folder from the Account list. For more information about accounts, see *Administering Oracle WebCenter Content*.
5. (Optional) To change the filer (or author) of the record folder from the default, select the user in the Filer field.
6. Enter a unique identifier.
7. Enter a name for the record folder.
8. (Optional) Enter a description of the folder.
9. (Optional) If the record folder is going to contain subject-to-review items:
    a. Select **Subject to Review**.
    b. Select a reviewer for notifications to override the system default set in the Configure Retention Settings page. The reviewer selected must have the Folder.EditReview right. Without that right, the reviewer cannot mark a record folder as reviewed.
    c. Enter the number and select type of period in the Review Period fields. If the category of a record folder is defined as subject to review, and a child record folder does not have its own review information defined, then the record folder inherits the review information from its category or its parent record folder. For further details, see Retention Schedule Attributes.
10. External information: If the item is external to the Records system, add its location, container, and applicable dates. For example, if an item has to do with a legal contract, the activation date represents the contract start date. The date format depends on user locale and preferences set in system properties. This field can also be used to treat a record folder and its content as a single piece of content from a disposition standpoint.

    You can also enter a deactivation date corresponding to a content item but external to the Records system. For example, if an item has to do with a legal contract, the expiration date represents the date the contract expires. This date differs from the expiration date for documents in the repository because the content can still be accessed in the Records system after deactivation. Content expired in Oracle WebCenter Content cannot be accessed after expiration.
11. Delete Approval Date: A date after which the folder can be deleted.
12. (Optional) To assign supplemental markings to the folder, select one or more markings from the Supplemental Markings list. Even if a user or group has permission to access a record folder, supplemental markings can still restrict record folder access.
13. (Optional, for ACL-enabled implementations) Set up ACL access at the alias level or user level.
14. Click **Lifecycle Preview** to view the disposition instructions associated with the category and thus the folder.
15. Click **Create**.

    The record folder is shown in the exploring retention category or record folder page.

12.4.2 Creating a Volume Folder

To create a volume folder within a retention category, or as a child folder of another record folder:

When a volume is created, all content in the folder is moved to a newly created volume folder. After the volume is created and content is moved, the folder is closed and cut off. Subsequent content items can be checked in to the parent folder, and additional volumes created for them.

> **Note:**
>
> The Folder.Create right is required to perform this action. This right is assigned by default to the Records Officer and Records Administrator roles.

Prerequisites

- Create a retention category
- Configure the time periods (for cycling items for review).
- Create a Supplemental Marking (optional)

This procedure also assumes security is configured and rights are assigned to users.

There are three methods to create a volume folder. This procedure describes two of those methods. See Creating a Volume Through Disposition for details about using dispositions to create volumes.

1. Open the retention category or record folder in which to create a volume folder.
2. Choose **Create** then **Create Volume** or **Schedule Volume Creation** from the page menu of a folder or a file plan folder (MoReq) containing only content.

   Create Volume creates the volume and inserts content immediately.

   Schedule Volume Creation opens a popup window where the volume creation can be scheduled depending on options selected:

   - The volume is created when a certain number of items is checked into the folder.
   - The schedule is checked when batch processes are executed and if matched, a volume is created and the content moved then.

12.4.2.1 Creating a Volume Through Disposition

When creating a disposition that has the **Create Volume** or the **Cutoff and Create Volume** action, slightly different actions occur.

If the **Create Volume** action is used, a volume is created. The content from the category or folder where the volume was created is then moved into the volume.

If the **Cutoff and Create Volume** action is used, the volume is created, and the content is moved and the volume is cut off from further processing.

12.4.3 Viewing Information

> **Note:**
>
> The Folder.Read right is required to perform these actions. All predefined management roles have this right.

Viewing folder information can be done in different ways depending on the location in the product hierarchy. First locate the item by browsing, searching, or screening. Then perform one of the following actions:

- On the search or screening results page, choose **Information** then the option (**Life Cycle**, **Recent Reviews**, and so on) from the folder's **Actions** menu.
- On the search or screening results page, click the **Info** icon of the folder.

  On the top menu on the Record Folder Information page, choose **Information** then the option needed (**Life Cycle**, **Metadata History**, and so on).

The information displayed depends on the configuration and if optional fields were populated.

12.4.3.1 Viewing Folder Life Cycle

Use the procedure described in Viewing Information to access the **Information** menu to view the life cycle (disposition schedule) of a record folder. The disposition instructions must be defined for the retention category of the folder. After a folder has been cut off, the record folder begins disposition processing and cannot be edited.

When **Life Cycle** is selected, the Life Cycle of Record Folder page opens.

The page shows the complete life cycle of the record folder according to its scheduled disposition, including the calculated dates of each disposition action if the trigger event has occurred.

12.4.3.2 Viewing a Folder Review History

Use the procedure described in Viewing Information to access the **Information** menu to view the review history of a record folder.

When **Recent Reviews** is selected, the Folder Review History page of the record folder opens.

The page shows a list of everyone who has reviewed the record folder and marked it as reviewed and the date and time of review.

12.4.3.3 Viewing Folder Metadata History

Use the procedure described in Viewing Information to access the **Information** menu to view the metadata history of a record folder. This is a list of all changes to the metadata of the record folder. When **Metadata History** is selected, the Metadata History of the record folder opens.

The page shows an overview of all changes made to the editable properties of the record folder and the affected metadata field name, the modification date and time, and the old and new values.

12.4.3.4 Viewing Folder Freeze Details

Use the procedure described in Viewing Information to access the **Information** menu to view detailed freeze information about a record folder (that is, a list of all freezes currently applied to the folder). When **Freeze Details** is selected, the Freeze Details page opens.

If the record folder is frozen, the **Freeze Disposition** field value is **Yes** on the Folder Information page and a **Details** link is displayed next to the field value. Click that link to view Freeze information.

The Freeze Details page shows all freezes currently applied to the record folder. If the folder inherited its freeze status from a parent folder, that folder's name is shown in the Inherited From column for the inherited freeze. Click the **Info** icon for an item in the list. The Record Folder Information page for the folder opens.

To save the information on this page to a file in the report, choose the **Save Freeze Details** option from the Page menu.

If the generated report file is in PDF format, it must be viewed using Adobe Acrobat version 6.0 or later.

12.4.4 Editing a Record Folder

Occasions on which a record folder would be edited include updating:

- A specific user access for ACL if alias/group permission is not used.
- A reason for freezing a record folder.
- Activation or expiration dates for internal content.
- Elaborating on or editing a folder description.
- The physical locations and containers for the physical counterpart of electronic items as they progress through their life cycle and are transferred to other locations.

To edit a record folder:

1. Navigate to the record folder to edit.
2. Choose **Edit** then **Record Folder** from the page **Actions** menu.
3. On the Create or Edit Record Folder page, make changes to the available fields.
4. Click **Submit Update**.

   The successfully updated folder message and the edits appear on the Record Folder Information page.
5. Click **OK**.

12.4.5 Changing the Disposition Applied to a Folder

To change the disposition instructions for a particular folder:

1. Navigate to the category that contains the folder to edit.
2. Choose **Edit** then **Edit Disposition** in the folder's **Actions** menu.
3. On the Disposition Instructions page, click the **Edit** icon (a pencil) in the row for the disposition to change.

   The Disposition Rule page opens.
4. Change the disposition rules as needed.
5. In the Advanced Options section, select the folder from the list. Specify to set the new disposition on content only, folders only, or on content and folders.
6. Click **OK** when done.

12.4.6 Moving a Record Folder

> **Note:**
>
> The Folder.Move right is required to perform this action. This right is assigned by default to the Records Officer and Records Administrator roles.

To move a record folder to a retention category or to another folder:

1. Navigate to the record folder to move.
2. Choose **Edit** then **Move** from the item **Actions** menu.
3. Click to expand the tree on the Select Retention Series, Record Folder or Category dialog and drill down in the hierarchy until reaching the category or folder where the record folder will be moved.

   The location field populates with the new location.
4. Click **OK**.

   The Exploring Category or Exploring Folder page and Browse Content area show the record folder in its new location.

12.4.7 Closing or Unclosing (Reopening) a Record Folder

After a record folder is closed, no further content can be checked (filed) into the closed record folder or its subfolders (child record folders) unless the user has the Folder.Open/Close right or is the author of the closed folder. If a user without these rights attempts to file content into a closed folder, a message is displayed stating the folder is closed. The content is not filed.

> **Note:**
>
> Closing a folder does not prevent disposition processing; only freezing a folder pauses disposition processing.

Closing a record folder refers to locking a record folder, and does *not* correlate with collapsing and expanding record folders within the Browse Content area. A closed or locked record folder is indicated with a padlock image superimposed on the record folder icon.

Depending on settings in a user's profile, the icons may appear slightly different, such as a book background icon rather a folder.

To close a record folder:

1. Access the **Edit** menu for the folder to close.
2. Select **Close**.

   A prompt appears to enter a reason for the action.
3. Enter the reason, or leave the text box empty.
4. Click **OK** to confirm. Click **Cancel** to end the entire action. If confirmed, the folder icon includes a padlock to indicate it is closed.

To unclose or unlock a folder, choose **Edit** then **Unclose** from the menu for the folder. Follow the same procedure as the one described to close a folder.

12.4.8 Freezing or Unfreezing a Record Folder

Freezing a record folder inhibits disposition processing for that folder. Frozen folders can still be browsed within the Browse Content area, content can be checked into frozen folders, and other edits as allowed by assigned rights can be done. Record folders residing in a frozen folder inherit the freeze status from their parent folder, but they can also be frozen independently of the folder (usually with a different freeze).

When freezing a record folder, choose from several predefined freezes and enter a reason for freezing the folder. The reason is shown in the Comments section of the audit trail, and in the Record Folder Information and Edit Record Folder pages. A frozen record folder is indicated by a pause symbol in the folder Name field of the Exploring Retention Category page.

More than one freeze can be applied to a record folder. View the Freeze Details page for the record folder to see a list of all freezes currently applied to the folder (both direct and inherited). See Managing Freezes for details about creating and viewing freezes.

To freeze a record folder:

1. Access the **Edit** menu for the folder to freeze.
2. Choose **Edit** then **Freeze** from the **Actions** menu.
3. On the Freeze/Unfreeze dialog, click the link to show all freezes and select the freeze to be applied. Provide a reason for the freeze or leave the text box empty.
4. Click **OK** to confirm the freeze. Click **Cancel** to abort the entire action.

   If confirmed, the freeze icon (two parallel vertical bars) appears next to the record folder name in the **Name** column of the Exploring page.

> **Note:**
>
> After a record folder is frozen, you cannot edit its freeze reason. If the freeze is no longer correct, you should unfreeze the folder and freeze it with a new reason.

Unfreezing a record folder releases a frozen folder again for disposition processing. Only one record folder at a time can be unfrozen. Follow the same procedure to unfreeze a folder, choosing **Edit** then **Unfreeze** from a menu. If the action is confirmed, the freeze icon no longer appears next to the record folder name in the **Name** column of the Exploring page.

12.4.9 Canceling, Expiring, and Rescinding Folders

> **Note:**
>
> The Folder.Edit right is required to perform these actions. This right is assigned by default to the Records Officer and Records Administrator roles.

Manipulating folders can be done in different ways depending on the location in the product hierarchy. First locate the folder by browsing, searching, or screening. Then perform one of the following actions:

- On the search or screening results page, choose **Set Dates** then the option (**Cancel**, **Expire**, and so on) from the folder's **Actions** menu.
- On the search or screening results page, click the **Info** icon of the folder.

  On the Record Folder Information page, on the top menu, choose **Set Dates** then the option needed.
- To perform actions on multiple folders, choose **Set Dates** then the option from the Table menu on the search result page.

You can undo these actions by choosing **Set Dates** then **Undo Obsolete** in the **Actions** menu for the folder or on the Page menu of the Record Folder Information page.

12.4.9.1 Canceling Folders

A record folder can be canceled directly, either after receiving a notification to do so (as part of a disposition instruction) or ad hoc. When a record folder is canceled, its status becomes obsolete.

1. Use the procedure described in Canceling, Expiring, and Rescinding Folders to access the **Set Dates** menu.
2. Choose **Cancel** from the **Set Dates** menu.

   A prompt appears to enter a reason for the action.
3. Enter a reason or leave the text box empty.
4. Click **OK** to confirm. Click **Cancel** to abort the entire action.

   The Record Folder Information page shows the date the record folder was canceled and also a corresponding obsolete date.

12.4.9.2 Expiring a Folder

A record folder can be expired directly, either after receiving a notification to do so (as part of a disposition instruction) or ad hoc. When a record folder is expired, its status becomes obsolete.

You can also expire a record folder if you are a records administrator processing pending events that receive notification.

1. Use the procedure described in Canceling, Expiring, and Rescinding Folders to access the **Set Dates** menu.
2. Select **Set Dates** then **Expire**.

   A prompt appears to enter a reason for the action.
3. Enter a reason or leave the text box empty.
4. Click **OK** to confirm. Click **Cancel** to abort the entire action.

   The Record Folder Information page shows the date the record folder was expired.

12.4.9.3 Rescinding a Folder

A record folder can be rescinded directly, either after receiving a notification to do so (as part of a disposition instruction) or ad hoc. When a record folder is rescinded, its status becomes obsolete.

1. Use the procedure described in Canceling, Expiring, and Rescinding Folders to access the **Set Dates** menu.
2. Choose **Set Dates** then **Rescind** from a menu.

   A prompt appears to enter a reason for the action.
3. Enter a reason or leave the text box empty.
4. Click **OK** to confirm. Click **Cancel** to abort the entire action.

   The Record Folder Information page shows the date the record folder was rescinded.

12.4.9.4 Making a Folder Obsolete

There are certain actions that automatically cause a record folder to become obsolete:

- Expire
- Cancel
- Rescind

You can also mark a folder as obsolete without using one of these actions. To mark a record folder obsolete:

1. Use the procedure described in Canceling, Expiring, and Rescinding Folders to access the **Set Dates** menu.
2. Choose **Set Dates** then **Obsolete**.

   A prompt appears to enter a reason for the action.
3. Enter a reason or leave the text box empty.

4. Click **OK** to confirm. Click **Cancel** to abort the entire action.

   The Record Folder Information page shows the date the record folder was made obsolete.

12.4.9.5 Reversing a Folder's Obsolete Status

The obsolete status of a record folder can be reversed. The status of expired, canceled, or rescinded record folders can be reversed.

> **Note:**
>
> The Folder.Edit right is required to perform this action. This right is assigned by default to the Records Privileged and Records Administrator roles.

Use the previously described procedure to access the **Set Dates** menu to reverse obsolete status.

1. Use the procedure described in Canceling, Expiring, and Rescinding Folders to access the **Set Dates** menu.
2. Choose S**et Dates** then **Undo Obsolete**.

   A prompt appears to enter a reason for the action.
3. Enter a reason, or leave the text box empty.
4. Click **OK** to confirm. Click **Cancel** to end the entire action.

12.4.10 Deleting a Record Folder

> **Note:**
>
> The Folder.Delete right is required to delete a record folder. This right is assigned by default to the Records Administrator role.

If a record folder has its own disposition rule or rules defined for it, deleting the record folder deletes the disposition rule from the category. To prevent the rule from being deleted, remove the association to the specific record folder.

To delete a record folder:

1. Open the retention category containing the record folder to delete.
2. Navigate to the record folder to delete.
3. Choose **Delete** then **Delete Record Folder** from the Item **Actions** menu.
4. You are prompted to confirm the deletion. Click **OK** to delete, or **Cancel** to cancel the deletion. To delete any child objects, select **Include child content items** on the prompt that appears. Click **Yes** when done.
5. You are prompted to enter a reason for the action. Enter a reason and click **OK** to confirm or leave the text box empty and click **OK**. Click **Cancel** to abort the entire action.

If confirmed, the record folder is deleted from the retention schedule.

12.4.11 Setting Dates with External Folders

> **Note:**
>
> The Folder.Edit right is required to perform these actions. This right is assigned by default to the Records Officer and Records Administrator roles.

An external record folder is external to the records management system, and has a tangible counterpart to the electronic record folder that tracks it. An external record folder is indicated on the Record Folder Information page by the information field External: Yes.

Setting dates can only be done on the Create or Edit Record Folder page. Use one of these methods to access that page:

- On the search or screening results page, choose **Edit** then **Edit Folder** from the folder's **Actions** menu.
- On the search or screening results page, click the **Info** icon of the folder.

  On the top menu of the Record Folder Information page, choose **Edit** then **Edit Folder** then the option needed.

12.4.11.1 Activating a Record Folder

To activate a record folder:

1. Use the procedure described in Setting Dates with External Folders to access the Create or Edit Record Folder page.
2. In the External fields area of the Create or Edit Record Folder page, click the calendar component icon and select a date for the **Activation date**.
3. Click **Submit Update**.

   The Record Folder Information page shows the activation date for the record folder.

12.4.11.2 Expiring a Record Folder

Entering an expiration date for a record folder also makes the folder have an obsolete status and date matching the expiration date.

To expire a record folder:

1. In the External fields area, click the calendar component icon and select a date for the **Expiration date**.
2. Click **Submit Update**.

   The Record Folder Information page shows the new date.

12.4.11.3 Entering a Delete Approval Date for an External Folder

You can enter an approval date for deleting at an external record folder from the retention schedule. Entering the delete approval date does not prevent deleting an external folder before that date. It only indicates the date when deleting the external folder was approved.

In the External fields area, click the calendar component icon and select a date for the **Delete Approval date**.

12.4.12 Classification Settings for Folders

The following tasks are performed when managing classification settings for record folders:

- Undoing a Record Folder Cutoff
- Marking a Record Folder as Reviewed
- Assigning Supplemental Markings to a Record Folder
- Removing Supplemental Marking from a Record Folder
- Applying a Specific Disposition Rule to a Record Folder

12.4.12.1 Undoing a Record Folder Cutoff

To undo (cancel) the cutoff of a record folder and make it available for disposition:

> **Note:**
>
> The Folder.UndoCutoff right is required to perform this action. This right is assigned by default to the Records Administrator role.

1. Browse content in the Retention Schedule to locate the appropriate record folder. Records administrators can use screening to quickly isolate record folders.
2. In the row of the folder, choose **Set Dates** then **Undo Cutoff** in the item's **Actions** menu.

12.4.12.2 Marking a Record Folder as Reviewed

Use this procedure to mark a record folder as reviewed in the Item Information page. Two commands are available:

- Mark reviewed
- Mark reviewed recursive

The Mark Reviewed action marks the current folder only as reviewed. Any child folders are not marked as reviewed. The Mark reviewed recursive action marks the current record folder being viewed as reviewed, with any child record folders and content. The **Mark reviewed recursive** option is only available if a record folder has child folders.

> **Note:**
>
> The Folder.Edit right is required to perform this action. This right is assigned by default to the Records Officer and Records Administrator roles.

1. Click **Browse Content** then **Retention Schedules**.

   The Exploring Series Retention Schedule page opens.
2. Navigate to the record folder to use and review the information.
3. In the row of the folder, choose **Set Dates** then **Mark Reviewed** (to mark only the current folder as reviewed) or **Mark reviewed recursive** (to mark all child folders and content as reviewed) from the folder's **Actions** menu.
4. You are prompted to enter a reason for the action. Enter a reason and click **OK** to confirm or leave the text box empty. Click **Cancel** to abort the entire action.

   The Record Folder Information page shows the date the record folder was reviewed.

12.4.12.3 Assigning Supplemental Markings to a Record Folder

To mark a record folder created with one or more supplemental markings, if it was not marked at initial folder creation:

Prerequisites

- Enabling Supplemental Markings
- Creating a Supplemental Marking
- Creating a Record Folder

> **Note:**
>
> The Folder.Edit right is required to perform this action. This right is assigned by default to the Records Officer and Records Administrator roles.

1. Click **Browse Content** then **Retention Schedules**.

   The Exploring Series Retention Schedule page opens.
2. In the row for the folder, choose **Edit** then **Edit Folder** from the folder's **Actions** menu.
3. On the Create or Edit Record Folder page, open the list in the **Supplemental Markings** field and click to select the marking or markings to associate with the record folder.
4. Click **Submit Update**.

   The successfully updated record folder message appears.

12.4.12.4 Removing Supplemental Marking from a Record Folder

> **Note:**
>
> The Folder.Edit right is required to remove a supplemental marking from a record folder. This right is assigned by default to the Records Officer and Records Administrator roles.

1. Click **Browse Content** then **Retention Schedules**.

   The Exploring Series Retention Schedule page opens.
2. Navigate to the record folder to use.
3. In the row of the folder, choose **Edit** then **Edit Folder** from the folder's **Actions** menu.
4. On the Create or Edit Record Folder page, delete a marking by editing the text in the **Supplemental Markings** text box.
5. Click **Submit Update**.

   A message appears, indicating the update was successful.

> **Note:**
>
> Each supplemental marking must have a comma and a space between markings, or else an Access Denied error occurs when trying to access content with multiple markings and when **Match All Markings** is enabled.

12.4.12.5 Applying a Specific Disposition Rule to a Record Folder

Use this procedure to apply a disposition rule within a retention category to a specific record folder only. This makes it possible to customize disposition instructions for a category with multiple record folders with slightly different disposition instructions.

Prerequisite

- Define the Disposition Instructions.

> **Note:**
>
> The Folder.Edit right is required to perform this action. This right is assigned by default to the Records Officer and Records Administrator roles.

To apply a disposition rule to a specific record folder:

1. Choose **Browse Content** then **Retention Schedules**.
2. On the Exploring page, navigate to the category that contains the record folder to use. In the top menu, choose **Edit** then **Edit Disposition**.

3. On the Disposition Instructions page, click the **Edit** icon (the pencil icon).
4. On the Disposition Rule page, change the disposition rules as needed. In the Advanced section, choose a folder from the **Apply to Record Folder** list (or the **On Folder(s)** list, if user-friendly captions are configured).

   The page closes. The record folder appears next to the rule.
5. You can further refine the disposition by selecting how the disposition is applied. Select an option from the **Disposition Applies To** list. Available choices are Content Only, Folders Only, or Content and Folders.
6. In the Disposition Instructions page, click **Submit Update**.

   The successfully updated dispositions message appears with the specific folder noted.

12.4.13 Folder Examples

The following examples demonstrate folder management tasks:

- Creating a Record Folder that is Subject to Review
- Creating Record Folders Subject to Recurring Audit Triggers

12.4.13.1 Creating a Record Folder that is Subject to Review

This example record folder has a three month review cycle. Editing a review cycle requires accessing a special edit page.

1. Open the retention category or record folder where the record folder will be created.
2. From the **Actions** menu, choose **Create Record Folder**.
3. On the Create or Edit Record Folder page, enter `RFV-101` as the Record Folder Identifier.
4. Enter `RFV-101` as the Record Folder Name.
5. Select **Subject to Review**.
6. Select a **Reviewer** to receive email notifications when it is time to review the record folder.
7. Enter `3 Months` as the Review Period.
8. Click **Create**.

   The record folder opens in the Exploring Retention Category page.
9. Click the **Info** icon for the new record folder.

   The Record Folder Information page displays Subject to Review: Yes and the corresponding Review Period. Any inherited review information from a parent record folder or from the retention category is also given.

12.4.13.2 Creating Record Folders Subject to Recurring Audit Triggers

This example demonstrates creating a record folder subject to the recurring audit trigger. The Audit Periods must already be defined in the Configuration Manager utility.

To create an audited record folder:

1. Open the retention category or record folder where the record folder will be created.
2. From the **Actions** menu, choose **Create Record Folder**.
3. On the Create or Edit Record Folder page, enter `RFA-101` as the Record Folder.
4. Enter `RFA-101` as the Record Folder Name box.
5. Select **Subject to Audit** and select an Audit Period from the list.
6. Click **Create**.

   The record folder appears in the Exploring page.
7. Click the **Info** icon for the new record folder.

   The Record Folder Information page displays Subject to Audit: Yes and the corresponding Audit Period.

13
Managing Security for Records

This chapter provides information on managing security for Oracle WebCenter Content: Records.
For information on administering Oracle WebCenter Content system security, including system-level roles, permissions, accounts, and ACLs, see Understanding Security and User Access in *Administering Oracle WebCenter Content*.

This chapter includes the following topics:

13.1 Understanding Records Security

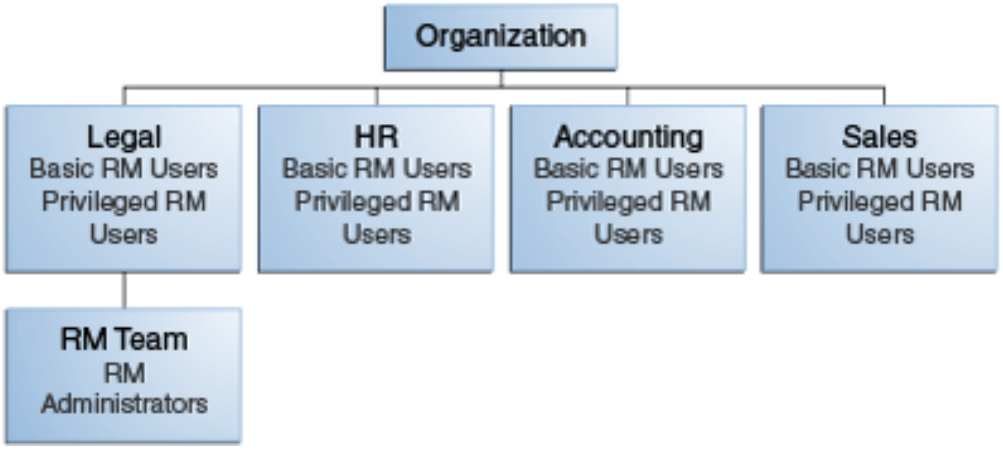
Multiple layers of security are available to control access to content. System security combined with security permissions and privileges for users allow you to customize the security easily. The intersection of all security mechanisms in place are used to determine user privileges with the strictest setting prevailing.

This section discusses the following topics:

13.1.1 Retention Management in an Organization

Figure 13-1 shows a typical retention management structure in an organization.

Figure 13-1 Typical Retention Management Organization



Most people in the various departments of an organization can file content or check in content items, search for items, and view them. These are basic Records Users.

A much smaller group of people is typically granted rights to perform some additional functions not allowed for basic users (for example, altering classifications or creating triggers or retention schedules). These are people with the Records Officer right.

A very limited number of people are administrators, who are typically responsible for setting up and maintaining the management infrastructure. Records Administrators have the widest range of rights to perform management tasks. For example, they can usually perform *all* and disposition actions, including those assigned to others. The administrators are often in the legal department of an organization, which can drive the efforts for effective and efficient management.

The software comes with predefined management roles called *rma*, *rmalocalrecordsofficer*, and *rmaadmin*, designated in the documentation as Records User, Records Officer, and Records Administrator. Each of these standard roles provides a default set of permissions and rights, which coincide with the typical responsibilities of basic users, privileged users, and administrators, respectively. These roles can easily be modified to suit specific management needs. New roles can be created with assigned management rights or different management rights can be given to existing roles.

Users without specific rights can still apply life cycles to content items.

> **Note:**
>
> Record management consists of more than just software. You also need to have the appropriate organizational structures and policies in place in your organization.

13.1.2 General Security Settings

Overall security settings are configured on the Configure Retention Settings page. The default values on that page are based on the installation level that was chosen.

Security preferences set on that page are in addition to those provided with Oracle WebCenter Content. PCM security is set using the Records security measures.

> **Note:**
>
> After a production environment is underway, it is recommended that the security settings for ACLs and other default settings not be changed. Doing so can cause unforeseen consequences.

To configure what security settings are enabled, choose **Records** then **Configure** then **Settings**.

- To use Access Control List Security, select **ACL-based security**.
- To activate the default security, select **Default Content Server security on Categories, Folders, and Triggers**.
- (Required for DOD 5015.2 compliance): To use supplemental markings, select **Supplemental Marking**. To make users match all supplemental markings, select **User must match all Supplemental Markings**. To allow a user to match only one supplemental marking, deselect the check box.
- To create custom security fields, select **Custom Security Fields**.
- To use classified security, select **Classified Security**.

When done, click **Submit Update**.

13.1.2.1 Security Groups

A security group defines security for a group of content. Oracle WebCenter Content: Records is shipped with a predefined security group called RecordsGroup. This group defines security for a group of content designated as that being tracked and/or retained.

Users with the predefined Records User, Records Officer, or Records Administrator roles have read and write permission (RW) to the RecordsGroup security group. Users with the Records Administrator role have read, write, delete, and admin permission (RWDA) to this security group.

> **Note:**
>
> Even though the default Records User and Records Officer roles appear to be identical, they are not. The default Records Officer role has subadministrator access to certain administrator functions that the default Records User role does not (for example, creating triggers and folders).

13.1.2.2 Aliases

When the product software is enabled, several aliases are created to help administrators manage large groups of people. Although the aliases are created, no default users are added to those groups. An administrator should add users as needed to the following alias lists:

- OffSiteRequestReviewGroup

- ReservationGroup
- RmaReviewersGroup

Several default aliases are also created if the FOIA/PA functionality is enabled. Default users are added to those alias lists but the users themselves are not created automatically. An administrator will need to create those users and assign appropriate permissions to them:

- FOIAOfficers
- FOIAProcessors
- FOIASpecialists
- JAG

13.1.2.3 Access Control Lists (ACLs)

> **Note:**
>
> Enabling or disabling ACLs affects existing ACL settings system-wide. For example, if ACLs are enabled in Oracle WebCenter Content and the Records system is configured to one of the DoD settings (which re-enables ACLs), the Oracle WebCenter Content ACLs are overridden. And if the **Typical** or **Minimal** Record settings are used, ACLs are disabled because ACL-based security is not enabled by default for those options. It is enabled by default for the DoD options.

ACLs control user and group access permissions for triggers, categories, and record folders. ACLs can be assigned for each category, folder, and trigger.

Be aware that searching for items takes more time when using ACLs as well as other security features, such as custom security fields and supplemental markings. When possible, use the default Oracle WebCenter Content security features and consider disabling ACLs for faster search retrieval performance.

Note that ACLs in the Records system behave differently than those in Oracle WebCenter Content in the following ways:

- Oracle WebCenter Content administrative users or users with the RWDA rights assigned to them have no automatic rights in the Records system. All users must have rights defined for them when using ACLs in the Records system.
- Oracle WebCenter Content: Records ACLs are hierarchical. If ACLs are enabled only in the Records system (and not in Oracle WebCenter Content), then ACLs are defined only on categories and folders, not directly on content. ACL rights are propagated down to content based on all rights assigned to the parent category or folder.

The `UseEntitySecurity` configuration variable is used to enable Oracle WebCenter Content ACL functionality. Set that variable to true to enable that feature.

The `SpecialAuthGroups` configuration variable is used to determine what security groups can be used with ACLs. For example, `SpecialAuthGroups=Private, RecordsGroup` enables those security groups to be used with ACLs. By default,

`RecordsGroup` is set as the SpecialAuthGroup value when Oracle WebCenter Content: Records is enabled.

13.1.2.3.1 Setting ACLs During Software Use

ACLs for individual users and groups and aliases can be adjusted while setting up elements of the Records system. Not all procedures allow the setting of all three types of permissions. The following procedure can be followed to adjust ACLs regardless of which type of permission are being set (user, group, or alias).

1. In the Group, User, or alias permission section of the Access Control Edit Section of the page in use, begin typing the user name of the person to add. A list appears and the user can be selected. Or type two asterisks (**) in the name field or group field. A list of users and groups appears.
2. Scroll to the name to use and click **Add User**, **Add Alias** or **Add**.
3. To the right of the name is a grouping of permissions. Click on a permission to add or remove it.
4. To remove a user or group from the permissions box, click the **X** next to the name.

13.1.3 Security Roles and Definitions

The following security elements are used to define user roles and permissions:

- Predefined user roles. Each role comes with a default set of permissions and rights, but these can be modified to suit specific needs. These include the following roles:
  - **rma**, generally assigned to basic users. It allows them to perform basic management tasks. In this documentation, Records User is a term used to designate the person given this role.
  - **rmalocalrecordsofficer**, generally assigned to users who need access to additional functionality (for example, creating triggers or folders, and modifying content attributes). In this documentation, Records Officer is a term used to designate a person given this role. In previous versions of this product, this was the Records Privileged role.
  - **rmaadmin**, generally assigned to administrators who set up and maintain the infrastructure and environment. In this documentation, Records Administrator is a term used to designate the person given this role.
  - **pcmrequestor**, generally assigned to users who have all the permissions of basic users without a PCM role but are also granted additional rights to perform some functions not allowed for basic users (for example, making reservations for physical items). Users with the pcmrequestor role have read and write permissions (RW) for the special RecordsGroup security group. In this documentation, PCM Requestor is a term used to designate a person given this role.
  - **pcmadmin**, generally assigned to administrators who are responsible for setting up and maintaining the physical content management infrastructure and environment. These users have the widest range of rights to perform physical content management tasks (for example, setting up the storage space, editing and deleting reservations, and printing user labels). Users with the PCM Administrator role have read, write, delete, and admin permissions (RWDA) for the special RecordsGroup security group. In this documentation, PCM Administrator is a term used to designate a person given this role.

- **Rights** control access to functions assigned to user roles. The predefined roles have a default set of rights assigned to them, but the rights can be modified to restrict or expand their access to functions.
- **Security groups** define security on a group of content. This software comes with a predefined security group called RecordsGroup. Users with the predefined Records User or Records Officer roles have read and write permission (RW) to the RecordsGroup security group. Users with the Records Administrator role have read, write, delete, and admin permission (RWDA) to this security group.
- **Access control lists** (ACLs) manage the security model on dispositions (ACLs are an optional feature available during configuration).ACLs can be assigned to folders, triggers, and retention categories. ACLs are used to control user and group access permissions for triggers, categories, and folders. The ACL can be assigned for each category, folder, and trigger that is created.

13.1.4 Rights and Roles for Records Tasks

Rights define what actions users can perform on content items. This section describes the default rights and roles for tasks involved in using Records. The default roles are **rma** (User), **rmalocalrecordsofficer** (Officer), and **rmaadmin** (Admin).

To assign rights to user roles:

1. Choose **Admin Applets** from the **Administration** menu.
2. Click the **User Admin** icon and choose **Security** then **Permissions by Role** from the menu.
3. Click the role to review or modify.
4. Click **Edit RMA Rights** then set the appropriate rights by selecting check boxes on the various tabs.
5. Click **OK** when done.

13.1.4.1 Triggers

The following table describes the default rights assigned to the default roles for tasks involving triggers.

Task	Required RM Right	User	Officer	Admin
View information about triggers	Admin.Triggers or Admin.RecordManager		X	X
Create a trigger	Admin.Triggers		X	X
Edit a trigger	Admin.Triggers		X	X
Delete a trigger	Admin.Triggers and Delete permission for the trigger's security group. The Delete permission is not granted by default.		X	X

13.1.4.2 Periods

The following table describes the default rights assigned to the default roles for tasks involving periods.

Task	Required RM Right	User	Officer	Admin
View information about periods	Admin.Triggers or Admin.RecordManager		X	X
Create a period	Admin.RecordManager			X
Edit a custom period	Admin.RecordManager			X
Delete a custom period	Admin.RecordManager			X

13.1.4.3 Supplemental Markings

The following table describes the default rights assigned to the default roles for tasks involving supplemental markings.

Task	Required RM Right	User	Officer	Admin
View information about supplemental markings	Admin.Triggers or Admin.RecordManager		X	X
Enable/disable supplemental markings	Admin.RecordManager			X
Create/edit a supplemental markings	Admin.RecordManager			X
Delete a supplemental marking	Admin.RecordManager			X

13.1.4.4 Security Classifications

The following table describes the default rights assigned to the default roles for tasks involving security classifications.

Task	Required RM Right	User	Officer	Admin
View information about classifications	Admin.RecordManager and Admin.SecurityClassifications			X
Enable/disable classifications	Admin.RecordManager and Admin.SecurityClassifications			X
Create/edit a classification	Admin.RecordManager and Admin.SecurityClassifications			X
Delete a classification	Admin.RecordManager and Admin.SecurityClassifications			X
Reorder security classifications	Admin.RecordManager and Admin.SecurityClassifications			X

13.1.4.5 Custom Security Fields

The following table describes the default rights assigned to the default roles for tasks involving security classifications.

Task	Required RM Right	User	Officer	Admin
View information about a custom security field	Admin.Triggers or Admin.RecordManager		X	X
Enable/disable custom security fields	Admin.RecordManager			X
Create/edit a custom security field	Admin.RecordManager			X

Task	Required RM Right	User	Officer	Admin
Delete a custom security field	Admin.RecordManager			X

13.1.4.6 Custom Category or Folder Metadata Fields

The following table describes the default rights assigned to the default roles for tasks involving custom metadata fields.

Task	Required RM Right	User	Officer	Admin
Create/edit a custom metadata field	Admin.RecordManager			X
Delete a custom metadata field	Admin.RecordManager			X

13.1.4.7 Classification Guides

The following table describes the default rights assigned to the default roles for tasks involving classification guides.

Task	Required RM Right	User	Officer	Admin
View information about classification guides	Admin.ClassificationGuide		X	X
Create/edit a classification guide	Admin.ClassificationGuide		X	X
Delete a classification guide	Admin.ClassificationGuide		X	X
View information about classification topics	Admin.ClassificationGuide		X	X
Create/edit a classification topic	Admin.ClassificationGuide		X	X
Delete a classification topic	Admin.ClassificationGuide		X	X

13.1.4.8 Freezes

The following table describes the default rights assigned to the default roles for tasks involving freezes.

Task	Required RM Right	User	Officer	Admin
View information about freezes	Admin.RecordManager			X
Create/edit a freeze	Admin.RecordManager			X
Delete a freeze	Admin.RecordManager and Delete permission for the freeze's security group. The Delete permission is not granted by default.			X
Send email notification about a freeze	Admin.RecordManager			X

13.1.4.9 Series

The following table describes the default rights assigned to the default roles for tasks involving series.

Task	Required RM Right	User	Officer	Admin
Browse and view information about freezes	Series.Read	X	X	X
Create/edit a series	Series.Create, Series.Edit			X
Delete a series	Series.Delete			X
Hide/unhide a series	Series.Hide, Series.Unhide			X
Move a series	Series.Move			X

13.1.4.10 Categories

The following table describes the default rights assigned to the default roles for tasks involving retention categories.

Task	Required RM Right	User	Officer	Admin
Browse and view information about retention categories, including disposition instructions	Category.Read	X	X	X
Create/edit a retention category	Category.Create, Category.Edit			X
Edit the review information for a retention category	Category.Edit.Review			X
Delete a category	Category.Delete			X
Apply disposition instructions to specific records in a category	Category.Edit			X
Move a category	Category.Move			X

13.1.4.11 Folders

The following table describes the default rights assigned to the default roles for tasks involving folders.

Task	Required RM Right	User	Officer	Admin
Browse and view information about folders	Folder.Read	X	X	X
View the life cycle of a folder, the review history of a folder and the metadata history of a folder	Folder.Read	X	X	X
Create a folder	Folder.Create		X	X
Edit a folder if author of the folder	Folder.EditIfAuthor		X	
Edit a folder if not author of the folder	Folder.Edit			X
Edit the review information for a folder	Folder.Edit.Review		X	X
Delete a folder	Folder.Delete			X
Move a folder	Folder.Edit			X
Close/unclose a folder	Folder.Open/Folder.Close		X	X
Freeze/unfreeze a folder	Folder.Freeze/Folder.Unfreeze			X

Task	Required RM Right	User	Officer	Admin
Cancel or expire a folder	Folder.Edit		X	X
Rescind or make a folder obsolete	Folder.Edit		X	X
Undo a folder's obsolescence status	Folder.Edit		X	X
Undo a folder's cutoff status	Folder.UndoCutoff			X
Review a folder	Admin.PerformPendingReviews		X	X
Mark a folder as reviewed	Folder.Edit		X	X
Set dates (activation, expiration, delete, and approval) for a folder	Folder.Edit		X	X
Assign or remove supplemental markings on a folder	Folder.Edit		X	X
Apply a disposition rule to one or many folders	Category.Edit			X

13.1.4.12 Content

The following table describes the default rights assigned to the default roles for tasks involving content.

Task	Required RM Right	User	Officer	Admin
Create or check in an item	Record.Create	X	X	X
Search for an item	Record.Read	X	X	X
Link items	Record.CreateLink	X	X	X
Unlink items	Record.Unlink		X	X
Download a content item for viewing	Record.Read	X	X	X
View information about content	Record.Read	X	X	X
View the life cycle of an item, the review history of an item, the classification history of an item or the metadata history of an item	Record.Read	X	X	X
Edit the review information for an item	Record.EditReview		X	X
Review the classification of an item	Record.Edit		X	X
Delete the metadata history of an item	Record.DeleteHistoryFile		X	X
Delete an item	Record.Delete			X
Freeze/unfreeze a folder	Record.Freeze/Record.Unfreeze			X
Cancel or expire an item	Record.Edit		X	X
Rescind or make an item obsolete	Record.Edit		X	X
Undo an item's obsolescence status	Record.Edit		X	X
Move an item to another category or folder.	Record.Edit		X	X
Edit record metadata before cutoff. **Note**: Non-record metadata can be edited after cutoff as well as before.	Record.UndoCutoff			X

Task	Required RM Right	User	Officer	Admin
Upgrade or downgrade an item's classification status	Record.Upgrade/Record.Downgrade		X	X
Review an item	Admin.PerformPendingReviews		X	X
Remove supplemental markings	Record.Edit		X	X
Undo the cutoff status of an item	Record.UndoCutoff			X
Undo the record status of an item	Record.UndoRecord			X

13.1.4.13 Disposition Rules

The following table describes the default rights assigned to the default roles for tasks involving disposition rules.

Task	Required RM Right	User	Officer	Admin
View disposition information	Category.Read	X	X	X
Enable/disable user-friendly captions	Admin.RecordManager			X
Create a rule	Category.Create			X
Edit a rule	Category.Edit			X
Delete a rule	Category.Delete			X
Define a custom disposition rule	Admin.CustomDispositionActions			
Disabling a disposition rule	Admin.CustomDispositionActions			

13.1.4.14 Archiving

The following table describes the default rights assigned to the default roles for tasks involving archiving.

Task	Required RM Right	User	Officer	Admin
Import an archive	Admin.RetentionSchedulesArchive and other rights for specific items in the import			X
Export an archive	Admin.RetentionSchedulesArchive and other rights for specific items in the export			X

13.1.4.15 Screening

The following table describes the default rights assigned to the default roles for tasks involving screening.

Task	Required RM Right	User	Officer	Admin
Enable/disable user-friendly captions	Admin.RecordManager			X
Screen a category, folder, or content	Any user can screen for items to which they have permission.			

13.1.4.16 Audit Trails

The following table describes the default rights assigned to the default roles for tasks involving audit trails.

Task	Required RM Right	User	Officer	Admin
Configure the audit trail	Admin.Audit			X
Choose metadata fields to audit	Admin.SelectMeta			X
Generate and view an audit trail	Admin.Audit			X
Search an audit trail or an archived audit trail	Admin.Audit			X
Set default metadata for audit trail check-in	Admin.Audit			X
Check in and archive audit trail	Admin.Audit, Admin.RecordManager			X

13.1.4.17 Links

The following table describes the default rights assigned to the default roles for tasks involving the configuration of links. Rights involved in using links are noted in Content.

Task	Required RM Right	User	Officer	Admin
Add a custom link type	Admin.ConfigureLinkTypes			X
Edit a custom link type	Admin.ConfigureLinkTypes			X
Delete a custom link type	Admin.ConfigureLinkTypes			X

13.1.4.18 Reports

The following table describes the default rights assigned to the default roles for tasks involving the configuration of reports.

Task	Required RM Right	User	Officer	Admin
Create a user, role, group, or user-group report	Admin.Reports			X

13.1.4.19 Customization

The Rma.Admin.Customization right is required to create custom dispositions, custom reports, or custom barcode actions. This right is not assigned by default to any role.

A detailed knowledge of services and their uses is required in order to customize your system.

13.1.4.20 General Configuration

The following table describes the default rights assigned to the default roles for tasks involving general product configuration.

Task	Required RM Right	User	Officer	Admin
Set the fiscal calendar	Admin.RecordManager			X
Perform disposition actions (process events)	Admin.RecordManager			X
Specify default review recipients	Admin.RecordManager			X

13.1.5 Rights and Roles for PCM Tasks

This section describes the rights and roles for tasks encountered while using Physical Content Management.

The default roles provided with PCM are **pcmrequestor** (Requestor) and **pcmadmin** (PCM Admin).

13.1.5.1 Physical Item Management

The following table describes the default rights assigned to the default roles for tasks involving physical items.

Note that the ability to freeze or screen physical items are not enabled by default for any role. The menu options to perform these tasks are not visible until those rights are assigned to a role.

Task	Required RM Right	Requestor	Admin
View information about physical items	PCM.Physical.Read and PCM.Storage.Read	X	X
Create (check in) a physical item	PCM.Physical.Create and PCM.Storage.Read	X	X
Edit a physical item	PCM.Physical.Edit and PCM.Storage.Read	X	X
Move a physical item	PCM.Physical.Edit, PCM.Physical.Move and PCM.Storage.Read		X
Delete a physical item	PCM.Physical.Delete and PCM.Storage.Read		X
Search physical items	PCM.Physical.Read and PCM.Storage.Read	X	X
Print labels for physical items	PCM.Admin.PrintLabel		X
Freeze or unfreeze physical items	Record.Freeze/Record.Unfreeze		
To manually override freeze errors	Admin.PerformActions		
To screen for physical items	Admin.Screening		

13.1.5.2 Storage Space

The following table describes the default rights assigned to the default roles for tasks involving storage locations.

Note that the ability to import a storage hierarchy is not enabled by default for any role. The menu option to perform this task is not visible until that right is assigned to a role.

Task	Required RM Right	Requestor	Admin
View information about locations	PCM.Storage.Read	X	X
Create a location	PCM.Storage.Create		X
Edit a location	PCM.Storage.Edit		X
Delete a location	PCM.Storage.Delete		X
Reserve a location	PCM.Storage.Reserve	X	X
Block a location	PCM.Storage.Block		X
Print labels for a location	PCM.AdminPrintLabel		X
Import batch-created storage hierarchy	Admin.RetentionScheduleArchive		

13.1.5.3 Location, Media, and Object Types

The following table describes the default rights assigned to the default roles for tasks involving the creation of location, media, and object types.

Task	Required RM Right	Requestor	Admin
Set up location types	PCM.Admin.Manager and PCM.Admin.LocationTypes		X
Set up object types	PCM.Admin.Manager		X
Set up media types	PCM.Admin.Manager		X
Set up custom metadata fields	PCM.Admin.Manager		X

13.1.5.4 Reservations

The following table describes the default rights assigned to the default roles for tasks involving reservations.

Task	Required RM Right	Requestor	Admin
View reservation information	PCM.Reservation.Read	X	X
Create a reservation request	PCM.Reservation.Create	X	X
Edit a reservation request	PCM.Reservation.Edit		X
Delete a reservation request	PCM.Reservation.Delete		X
Process a reservation request	PCM.Reservation.Process		X
Run a reservation request report	PCM.Admin.Manager		X
Configure default metadata for reservations	PCM.Admin.Manager		X

13.1.5.5 Chargebacks

The following table describes the default rights assigned to the default roles for tasks involving chargebacks.

Task	Required RM Right	Requestor	Admin
Set up chargeback types, payment types, and customers	PCM.Admin.Manager and CBC.ChargeBacks.Admin		X
View information about chargebacks (transactions, invoices, and so on)	PCM.Admin.Manager, CBC.ChargeBacks.Admin and CBC.ChargeBacks.Read		X
Create chargeback items (transactions, invoices, and so on)	PCM.Admin.Manager, CBC.ChargeBacks.Admin and CBC.ChargeBacks.Read		X
Edit chargeback items (transactions, invoices, and so on)	PCM.Admin.Manager, CBC.ChargeBacks.Admin and CBC.ChargeBacks.Edit		X
Delete chargeback items (transactions, invoices, and so on)	PCM.Admin.Manager, CBC.ChargeBacks.Admin and CBC.ChargeBacks.Delete		X
Screen for charges	PCM.Admin.Manager and CBC.ChargeBacks.Admin		X
Browse invoices	PCM.Admin.Manager and CBC.ChargeBacks.Admin		X
Print invoices	PCM.Admin.Manager and CBC.ChargeBacks.PrintInvoice		X
Adjust invoices	PCM.Admin.Manager and CBC.ChargeBacks.Adjust		X

13.1.5.6 Barcodes

The following table describes the default rights assigned to the default roles for tasks involving barcodes and barcode labels.

Task	Required RM Right	Requestor	Admin
Process barcode files	PCM.Barcode.Process		X
Print labels for users, storage locations, and physical locations	PCM.Admin.PrintLabel		X

13.1.5.7 General Configuration

The following table describes the default rights assigned to the default roles for tasks involving general configuration options.

Task	Required RM Right	Requestor	Admin
Configure the PCM environment	PCM.Admin.Manager		X
Run batch services	PCM.Admin.Manager		X

13.1.6 External Source Tasks and Defaults for Predefined Roles

For more information about adapters, see Managing the Oracle WebCenter Content Records Adapter.

The following rights are required to perform the following tasks:

- To read external items, the ECM.External.Read right is required. This right is assigned by default to the ERM Requestor and ERM Administrator roles.
- To create an external item, the ECM.External.Create right is required. This right is assigned by default to the ERM Requestor and ERM Administrator roles.
- To edit an external item, the ECM.External.Edit right is required. This right is assigned by default to the ERM Administrator role.
- To delete an external item, the ECM.External.Delete right is required. This right is assigned by default to the ERM Administrator role.
- To perform administrative functions involving the external source, the ECM.External.Admin right is required. This right is assigned by default to the ERM Administrator role.

13.1.7 Permissions Matrix

The table below shows a matrix of content and retention schedule components, and the corresponding permissions for each predefined role. Supplemental markings have the most restrictive access capabilities.

Objects and Retention Schedule Components	Subject to Additional Security of Type	Records User (rma)	Records Officer (recordsofficer)	Records Administrator (rmaadmin)
Content Items	Rights; supplemental markings; custom security field; ACLs	RW	RW	RWDA
Folders	Rights; supplemental markings; ACLs	R	RWD	RWD
Categories	Rights; supplemental markings; ACLs	R	R	RWD
Series	Rights; ACLs	R	R	RWD
Triggers	Rights; ACLs		RW RWD permission required to delete triggers.	RWDA Only custom triggers can be deleted.
Periods	Rights		R	RWD Only custom periods can be deleted.
Supplemental markings	Rights			RWD
Classification guides	Rights			RWD

13.2 Setting Security Preferences

Security preferences are set on the Configure Retention Settings page. The security preferences set on that page are in addition to those provided with Oracle WebCenter

Content. The available security depends on what type of installation was chosen (for example, Minimal or a DoD setting).

> **Note:**
>
> After your production environment is underway, it is recommended that you do not change the security settings for ACLs or the default security.

To configure security setting:

1. Choose **Records** then **Configure**.
2. Choose **Retention** then **Settings**.
3. On the Configure Retention Settings page, click the plus icon (+) to expand the Security section on the page.
4. (Optional based on the security model): To make use of Access Control List Security, select **ACL-based security**. This is enabled by default when DoD Baseline or DoD Classified is enabled.
5. (Recommended): To activate the default security inherent in Universal Content Management for extra security on categories, folders, and triggers, select **Default Content Server security on Categories, Folders, and Triggers**.
6. (Required for DOD 5015.2 compliance): To use supplemental markings, select **Supplemental Marking**.
7. (Optional based on the security model): To make users match all supplemental markings on a record folder, select **User must match all Supplemental Markings**. This is the most restrictive setting for supplemental markings. To allow a user to match only one supplemental marking to a folder to access its content or a content item (in the case of multiple supplemental markings), deselect the box.
8. (Optional): To create custom security fields at the content field level to further restrict users, select **Custom Security Fields**.
9. (Optional): To use classified security, select **Classified Security**. For more information, see Classified Security.
10. Click **Submit Update**.

    A message appears indicating the settings have been configured successfully.

> **Note:**
>
> Items created for use in the Retention Schedule must have the security group set to recordsgroup rather than Public. If the security group is set to Public, non-URM users might have access to items in the Retention Schedule when performing standard searches.

13.3 Assigning Rights to User Roles

The system is shipped with several predefined roles. Each of these roles has several default rights, which define what users with that role are allowed to do.

Some of the rights are interconnected. Enabling or disabling certain options automatically enables or disables other options. For example, if you disable the **Record.Create** option on the **Record** tab, some of the other options on that tab are disabled as well. Conversely, if you enable the **Category.Create** option on the **Category** tab and the **Category.Read** option is not yet enabled, it is enabled automatically.

The following sections describe the tabs where rights appear:

- Series Tab
- Category Tab
- Folder Tab
- Record Tab
- Admin Tab
- CBC Tab
- PCM Tab
- ECM Tab
- Setting Rights for Roles

13.3.1 Series Tab

The following rights appear on the **Series** tab of the Edit Rights page:

- Read: Allows the user to view information about a series. It is assigned by default to the Records User, Records Officer, and Records Administrator roles.

The following rights are assigned by default to the Records Administrator role.

- Create: Allows the user to create a series.
- Delete: Allows the user to delete a series.
- Move: Allows the user to move a series.
- Edit: Allows the user to edit a series.
- Hide/Unhide: Allows the user hide and unhide a series.

13.3.2 Category Tab

The following rights appear on the **Category** tab of the Edit Rights page.

- Read: Allows the user to view information about a retention category. It is assigned by default to the Records User, Records Officer, and Records Administrator roles.

The following rights are assigned by default to the Records Administrator role:

- Create: Allows the user to create a retention category.
- Delete: Allows a user to delete a retention category.
- Move: Allows a user to move a retention category.
- Edit: Allows a user to edit a retention category.
- Edit Review: Allows a user to edit a retention category that is subject to review.

13.3.3 Folder Tab

For more information about folders, see Managing Folders.

The following rights appear on the **Folder** tab of the Edit Rights page:

- Read: Allows the user to view information about a folder. It is assigned by default to the Records User, Records Officer, and Records Administrator roles.
- EditIfAuthor: Allows a user to edit a folder, but only if the user is the author of that folder. It is not assigned by default to any role.

The following rights are assigned by default to the Records Officer and Records Administrator roles:

- Create: Allows a user to create a folder.
- Open/Close: Allows a user to open or close a folder.
- Edit Review: Allows a user to edit a folder that is subject to review.
- Move: Allows a user to move a folder.

The following rights are assigned by default to the Records Administrator role:

- Edit: Allows a user to edit a folder, even if the user is not the author of that folder.
- UndoCutoff: Allows a user to undo the cutoff of a folder.
- Delete: Allows a user to delete a folder.
- Freeze/Unfreeze: Allows a user to freeze and unfreeze a folder.

13.3.4 Record Tab

The following rights appear on the **Record** tab of the Edit Rights page. These rights are assigned by default to the Records User, Records Officer, and Records Administrator roles:

- Read: Allows the user to view information about an item.
- CreateLink: Allows the user to link content items.
- Create: Allows a user to create content or check it in to the retention schedule.
- Unlink: Allows a user to unlink content.

The following rights are assigned by default to the Records Officer, Records User, and Records Administrator roles:

- Edit: Allows the user to edit content, including moving, canceling, expiring, rescinding, making obsolete, and reviewing.
- EditReview: Allows a user to edit content that is subject to review.
- DeleteHistoryFile: Allows a user to delete the metadata history file of content. This option is only available if the Classified Security option is enabled.
- Upgrade/Downgrade: Allows a user to upgrade and downgrade the security classification of content. This option is only available if the Classified Security option has been enabled on the Configure Retention Settings page.

The following rights are assigned by default to the Records Administrator role:

- UndoCutoff: Allows a user to undo the cutoff of an item.

- Delete: Allows a user to delete content within the retention schedule.
- Freeze/Unfreeze: Allows a user to freeze and unfreeze content.
- UndoRecord: Allows a user to undo the status of content.

13.3.5 Admin Tab

The following rights appear on the **Admin** tab of the Edit Rights page.

- PerformPendingReviews: Allows a user to perform pending reviews. This right is assigned by default to the Records Officer, Records User, and Records Administrator roles. See Assigning Rights to User Roles.
- PrivilegedEnvironment: Allows a user to set the de-classification time frame. For details, see Assigning Rights to User Roles. This right is assigned by default to the Records Officer and Records Administrator roles. This option is only available if the Classified Security option has been enabled on the Configure Retention Settings page.
- ClassificationGuide: Allows a user to work with classification guides. This right is assigned by default to the Records Officer and Records Administrator roles.
- Triggers: Allows the user to work with global triggers, custom direct triggers, and indirect triggers. For details, see Assigning Rights to User Roles. To delete a trigger, Delete permission (D) for the trigger's security group is also required. This right is assigned by default to the Records Officer and Records Administrator roles.
- ShareFavorites: Allows users to share the contents of their Favorites list with other users. This right is assigned by default to the Records Officer and Records Administrator roles.

The following rights are assigned by default to the Records Administrator role:

- RecordManager: Allows a user to configure several settings and also set up and administer periods, supplemental markings, security classifications, custom security fields, custom category and folder metadata fields, classification guides and freezes.
- Screening: Allows a user to screen retention categories, folders, and content.
- PerformActions: Allows a user to process content assignments.
- SelectMeta: Allows a user to specify metadata fields to be audited.
- Reports: Allows a user to generate user and group reports.
- RetentionScheduleArchive: Allows a user to import and export a retention schedule archive.
- SelectAuthor: Allows a user to select a different filer (author) for a category than him/herself.
- Audit: Allows a user to work with audit trials.
- ConfigureLinkTypes: Allows a user to manage custom content links.
- AllowDispositionUpgrade/Downgrade: Allows a user to perform upgrade and downgrade classification actions.

The following rights *are not assigned* by default to any role.

- NoPostFilterSearch: Allows users to unfilter search results. The results include content the user has no access to based on security classifications, supplemental markings, custom security fields, and ACLs. If the user has no access to a content item in the search results, clicking on it results in an access denied error. By enabling this option, search queries are executed much faster because no complex post-filtering must be performed.

  Users with this right can still only access content items they have been explicitly granted access privileges to based on security groups and accounts. They will see other results in the search results list, but cannot access them. They may also see some metadata information about the content item (for example, their title), which may interfere with an organization's security model.
- NoSecurity: Allows users to become immune to security classifications, supplemental markings, custom security fields, and ACLs. Their access to content is unrestricted by these security features. In addition, this option turns off search post-filtering, so search results include content the user has not been explicitly granted access to. For example, a user would have access to content marked as Top Secret even if that security classification has not been assigned to the user. This right can be used to give system administrators the privilege to access every content item in the system.

  Access to content items continues to be restricted by security groups and accounts.
- Customization: Allows users to define custom disposition actions or to delete any disposition action. Also allows users to define custom reports.
- SecurityClassifications: *new installs only.* If enabled (with the Admin.RecordManager option), the user is allowed to set up security classification levels. This option is only available if the Classified Security option is enabled.
- GetAllFilePlan: Allows a user to get all series, categories, and folders when the GET_FILE_PLAN_ALL service is called. Without this right, inaccessible objects are excluded. The service is typically used by adapters.

> **Note:**
>
> When a user has Admin permission to a security group but does not have the Admin.SelectAuthor right, the user is still able to select an author at checkin. The Admin.SelectAuthor right is used only to add that functionality to a user who does not have Admin permission to a group.

13.3.6 CBC Tab

Chargebacks are used with Physical Content Management, which is only available when that software is enabled.

The following rights are assigned by default to the PCM Administrator role:

- ChargeBacks.Read: Allows the user to view information about chargeback-related items (transactions, invoices, and so on).
- ChargeBacks.Create: Allows a user to create chargeback-related items.
- ChargeBacks.Edit: Allows a user to edit chargeback-related items.
- ChargeBacks.Delete: Allows users to delete chargeback-related items.
- ChargeBacks.PrintInvoices: Allows users to print invoices.

- ChargeBacks.MarkPaid: Allows users to mark invoices as paid.
- ChargeBacks.Adjust: Allows users to manually adjust invoices.
- ChargeBacks.Admin: Allows users to perform administrative tasks such as define new payment types, define customers, and so on.

13.3.7 PCM Tab

The following rights are assigned by default to the PCM Requestor and PCM Administrator roles:

- Physical.Read: Allows the user to view information about physical items.
- Physical.Create: Allows a user to create physical items.
- Physical.Edit: Allows a user to edit physical items.
- Storage.Read: Allows users to view information about a storage location.
- Storage.Reserve: Allows users to reserve a storage location.
- Reservation.Read: Allows users to view information about reservations.
- Reservation.Create: Allows users to create reservations.
- Reservation.Edit: Allows users to alter reservations.

The following rights are assigned by default to the PCM Administrator role only:

- Physical.Move: Allows users to move a physical item (change the location)
- Physical.Delete: Allows users to delete physical items.
- Storage.Create: Allows users to create new storage.
- Storage.Edit: Allows users to edit an existing storage location.
- Storage.Delete: Allows users to delete a storage location.
- Storage.Block: Allows users to block or unblock a storage location.
- Reservation.Delete: Allows users to delete reservations.
- Reservation.Process: Allows users to process reservations by modifying the status of request items.
- Barcode.Process: Allows users to process barcode files.
- Admin.Manager: Allows a user to access all PCM administrative functions.
- Admin.Location.Types: Allows users to configure location types, providing the user also has the Admin.Manager right.
- Admin.PrintLabel: Allows users to generate labels for users, locations, and physical items.

13.3.8 ECM Tab

The following rights are assigned by default to the ERM Requestor and ERM Administrator roles:

- External.Read: Allows the user to view information about external items.
- External.Create: allows a user to create external items.
- External.Edit: allows a user to edit external items.

The following rights are assigned by default to the ERM Administrator role only:

- External.Delete: allows users to delete external items.
- External.Admin: allows users to perform administrative tasks.

13.3.9 Setting Rights for Roles

Rights define what actions users are allowed to perform. To assign rights to user roles:

1. Choose **Admin Applets** from the **Administration** menu.

   The Administration Applets for the server appears.
2. Click the **User Admin** icon.

   The User Admin utility starts.
3. Choose **Security** then **Permissions by Role** from the menu.
4. Select the role to review or modify. Click **Edit RMA Rights** or **Edit ECM Rights** for PCM.
5. On the Edit Rights page, set the rights by selecting check boxes on the various tabs.
6. Click **OK** when done.
7. Click **Close** to exit the Permissions by Role page.

13.4 Specifying PCM Barcode Values for Users

Barcodes are used with Physical Content Management, which is only available when that software is enabled.

By default, the barcode value for a user consists of a user's login name in all upper-case letters, for example `JSMITH` or `MJONES`. If you do not want to use the login name of a user as the barcode value, use the User Admin utility to specify a different value for the user.

This is especially useful for login names containing characters other than the basic letters (a-z, A-Z) or numbers (0-9) (for example, accented letters such as `kmüller`). By default, the barcode values generated for such users include hexadecimal representations of the accented letters (for example, `KMC39CLLER`). To avoid this behavior set specific barcode values for these users (for example, `KMULLER`), which are then used rather than the (converted) user login names.

You can run the `Update Users with no Barcode` batch service to automatically set the barcode values for all users who currently do not have a barcode value. This is useful for users who are already in the system before Physical Content Management was enabled. The barcode values are set in accordance with the rules above.

To manually set a specific barcode value for a user:

1. Log in as an administrator.
2. Click **Administration** then click **Admin Applets**.
3. Click the **User Admin** icon.

   The User Admin utility starts.
4. On the **Users** tab, select the user whose barcode value should be set and click **Edit**.

5. In the Edit User dialog in the **Barcode** field, specify a unique value for the user. This value is used in the barcode label for the user rather than the user's login name (in all upper-case letters) as specified in the Name field.

   The specified value must be unique for each user in the system. An error message is displayed if a value is used that is not unique.

   Do not use any accented letters in the barcode value (an error message is displayed if you try). Also, any lower-case letters are automatically converted to upper case after clicking **OK**.

6. Click **OK** when finished.
7. Close the User Admin utility.

13.5 Classified Security

The classification of content is the process of identifying and safeguarding content requiring protection against unauthorized disclosure, for example, because it contains information sensitive to the national security of the United States or sensitive to the stability of a company.

Classifications, supplemental markings, and classification guides provide further security and are used to organize documents that are considered classified, for either government or corporate purposes.

The following sections discuss classified security:

- Security Classifications
- Managing Security Classifications
- Classification Guides
- Managing Classification Guides
- Supplemental Markings
- Managing Supplemental Markings

13.5.1 Security Classifications

Security classification can be an additional way to restrict access to content by using supplemental markings and custom security fields.

Several classification features are available to handle and process classified content in accordance with the Chapter 4 requirements of the DoD 5015.2 specification. Several built-in classifications (Top Secret, Secret, and Confidential) are available, but custom classifications can also be created.

Content is either classified, unclassified, or declassified. **Classified** content has an initial classification and a current classification. **Unclassified** content is not and has never been classified. **Declassified** content was formerly classified.

The standard security categories (classification scheme), from highest to lowest, are **Top Secret**, **Secret**, **Confidential**, and **No markings** (that is, unclassified).

Like supplemental markings, classified security can be enabled or disabled at any time. After enabling, custom security classifications can be created. If any additional security classifications are created, indicate the classification place within the marking hierarchy.

To enable security, select **Classified Security** on the Configure Retention Settings page. Click **Submit**.

> **Caution:**
>
> Disabling classified security puts sensitive classified information at risk of being accessed by unauthorized people. After your classified security is in force, it is recommended that you do not disable it.

Custom classifications can also be defined. For details, see Creating Custom Security Classification.

The following descriptions are applicable for those companies that are using the Oracle WebCenter Content: Records product for DoD compliance.

When using security classification for corporate use only (that is, if you are not concerned with DoD compliance), these terms can be defined as necessary for the organization's infrastructure. For example, Top Secret may apply to content that is critical to the operation of your company and should never be deleted, while Confidential may apply to content that must be kept limited to a specific group of individuals, such as Human Resource representatives or members of your accounting team.

Figure 13-2 Classified Hierarchy

13.5.1.1 Top Secret

If complying with DoD Section 1508, the Top Secret classification (according to Executive Order 12958) is "applied to information, the unauthorized disclosure of which could be expected to cause *exceptionally grave damage* to the national security that the original classification authority is able to identify or describe."

If complying with DoD Section 1508, only the President of the United States has the authority to classify content as Top Secret, pursuant to the Executive Order 12958. For further details, access the following link:

http://www.fas.org/sgp/clinton/eo12958.html

13.5.1.2 Secret

According to EO 12958, the Secret classification level is "applied to information, the unauthorized disclosure of which could be expected to cause *serious damage* to the national security that the original classification authority is able to identify or describe."

13.5.1.3 Confidential

According to EO 12958, the Secret classification level is "applied to information, the unauthorized disclosure of which could be expected to cause *damage* to the national security that the original classification authority is able to identify or describe."

13.5.1.4 Classification Levels

The standard security categories (classification scheme), from highest to lowest, are as follows:

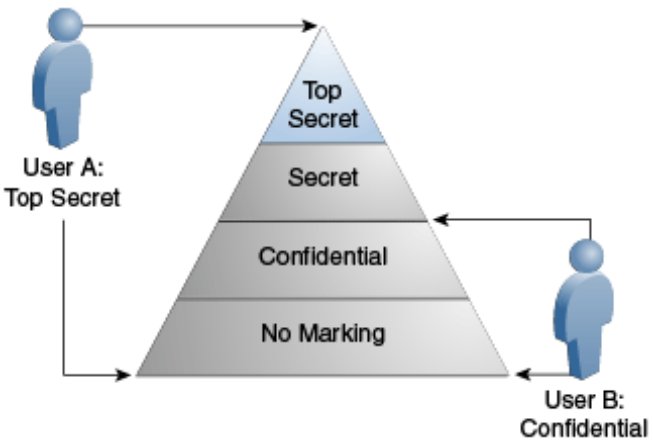
1. Top Secret
2. Secret
3. Confidential
4. No markings (unclassified)

13.5.1.5 Classified Records Security Hierarchy

Every retention user has access to unclassified content, provided all other security criteria are met (such as supplemental markings, right, roles, and so on).

A user who has access to Top Secret classification has access to all lower classifications as well, as shown for User A in Figure 13-3. User B has access to Confidential content and unclassified content.

Figure 13-3 Hierarchical User Access



13.5.2 Managing Security Classifications

When using classified security, you must first set the classifications to be used. Then set the time frame for classifying and declassifying, then lastly assign classification ability to different users. The following tasks are discussed in regard to managing classifications:

- Enabling or Disabling Classified Security
- Creating Custom Security Classification
- Editing a security classification
- Setting the Order of Security Classifications
- Deleting a Security Classification
- Setting the Declassification Time Frame
- Viewing Security Classification References
- Assigning a Classification to a User
- Changing a User's Classification
- Removing a User's Classification

13.5.2.1 Enabling or Disabling Classified Security

You can enable and disable classified security at any time. Enabling classified security enforces the security classifications assigned to users who attempt to access classified data. It is not recommended that classified security be disabled after it has been in use.

After enabling classified security, create any custom security classifications required by the organization. If additional security classifications are created, make sure to indicate the classification's place within the marking hierarchy. For further information, see Setting the Order of Security Classifications.

> **Note:**
>
> The Admin.RecordManager right is required to perform this action. This right is assigned by default to the Records Administrator role.

1. Choose **Records** then **Configure** then **Settings**.
2. Expand the Security section on the Configure Retention Settings page. Select **Classified Security**.
3. Click **Submit**.

   A message appears stating the configuration was updated successfully.

> **Caution:**
>
> Disabling classified security puts sensitive classified items at risk of being accessed by unauthorized people. After your classified security is in force, it is recommended that you do not disable it.

To disable classified security:

1. Choose **Records** then **Configure** then **Settings**.
2. On the Configure Retention Settings page, deselect **Classified Security**.
3. Click **Submit**.

   A message appears stating the configuration was updated successfully. Classified security is now disabled and the security classification selection field is hidden from view on the content check-in form.

13.5.2.2 Creating Custom Security Classification

Use this procedure to create a new security classification. After creating a custom classification, indicate its order in the hierarchy. If not done, the security classification is ignored. For further information, see Setting the Order of Security Classifications.

Security classifications can be created only if the classified security feature has been enabled.

When editing an existing security classification, the description can be modified but not its name.

> **Note:**
>
> The Admin.RecordManager and Admin.SecurityClassifications rights are required to perform these actions. These rights are assigned by default to the Records Administrator role.

1. Choose **Records** then **Configure**.
2. Choose **Security** then **Security Classification**.
3. On the Configure Security Classification page, click **Add**.
4. On the Configure Security Classification page, enter a name for classification with a maximum length of 30 characters.
5. Enter a description if needed. Maximum length is 30 characters.
6. Click **Create**.

   A message appears indicates creating the classification was successful.
7. Click **OK**.

   The Configure Security Classification page opens with the new classification in the list. A user must be assigned the classification level or a higher level to be able to view the security classification level. Make sure to indicate the placement of the

new classification in the hierarchy. For further information, see Setting the Order of Security Classifications.

> **Note:**
>
> When editing a classification, you must also be assigned the highest security level to view all of the available classifications for editing.

13.5.2.3 Editing a security classification

To edit an existing security classification:

1. Choose **Records** then **Configure**.
2. Choose **Security** then **Security Classification**.
3. On the Configure Security Classification page, click the **Edit** icon (a pencil) next to the classification to edit.
4. On the Create or Edit Security Classification page, make any changes to the description and click **Submit Update.**

   A message appears stating the security classification was updated successfully.
5. Click **OK**.

13.5.2.4 Setting the Order of Security Classifications

Prerequisites

- Create any custom security classifications that are required. Assign yourself the highest classification level so you can view and reorder all levels.

> **Note:**
>
> The Admin.RecordManager and Admin.SecurityClassifications rights are required to perform this action. These rights are assigned by default to the Records Administrator role. You must also have the specific security classification level assigned to you to view or work with it.

Use this procedure to indicate the order of the security classifications within the security classification hierarchy. If only the built-in security classifications are used in their default order, this procedure is not needed.

1. Choose **Records** then **Configure**.
2. Choose **Security** then **Security Classification**.
3. Use the **Up** or **Down** arrow on the Configure Security Classification page to move a selected security classification in the classification hierarchy. The highest classification should be at the top of the list and the lowest at the bottom.

> **Note:**
>
> The last item in the list will be unclassified regardless of the name you assign to it. Make sure you have a classification in your hierarchy that you intend to be designated as unclassified.

4. Click **Submit Update**.

   A message appears stating the configuration was updated successfully.

13.5.2.5 Deleting a Security Classification

A classification cannot be deleted until any references to the classification in content are removed. Security classification assignments must also be manually removed from users. If you attempt to delete a security classification still in use, a message is displayed stating the classification is in use by users (it is assigned to users and must be removed) or by content.

Search for security classifications from the Search page. Use the search results to see which items have the classification in use. Screening can also be used to quickly isolate content.

> **Note:**
>
> The Admin.RecordManager and Admin.SecurityClassifications rights are required to perform this action. These rights are assigned by default to the Records Administrator role. You must also be assigned the highest security level to view all of the available classifications for deleting.

1. Choose **Records** then **Configure**.
2. Choose **Security** then **Security Classification**.
3. On the Configure Security Classification page, click the **Delete** icon (a red X) next to the classification to delete.

   A message appears stating the security classification was deleted successfully.
4. Click **OK**.

13.5.2.6 Setting the Declassification Time Frame

Classified items are automatically declassified after 25 years unless they were exempted from declassification. When an item is declassified, the Declassify On Date field is compared to the Publication Date, and if the retention period for classification status exceeds ten years, an alert is presented to the user.

> **Note:**
>
> The Admin.PrivilegedEnvironment right is required to perform this action. This right is assigned by default to the Records Officer and Records Administrator roles.

1. Choose **Records** then **Configure** then **Settings**.
2. Expand the **Classified Topics** area of the Configure Retention Settings page. In the **Maximum Years Before Declassifying** field, enter the number of years after which items will be declassified. The default is 25. If this field is not available, the Admin.PrivilegedEnvironment right is not assigned to the user viewing the page.

   If this field is set to 0 and auto-computation of declassification dates is chosen, any classified items currently in the system are set to declassified.
3. Click **Submit Update**.

   A message appears stating the configuration is successful.
4. Click **OK**.

13.5.2.7 Viewing Security Classification References

Use this procedure to view references to a security classification (those disposition rules that use the security classification in their definitions).

> **Note:**
>
> The Admin.RecordManager and Admin.SecurityClassifications rights are required to perform this action. These rights are assigned by default to the Records Administrator role. You must also be assigned the highest security level to view all of the available classifications for viewing.

1. Choose **Records** then **Configure**.
2. Choose **Security** then **Security Classification**.
3. On the Configure Security Classification page, select the security classification to view and click **Info.**
4. On the Security Classification Information page, choose **Reference** from the page menu.

   If any of the content links are clicked, the associated content information page for that item opens.

13.5.2.8 Assigning a Classification to a User

You can assign security classifications only if the classified security feature has been enabled.

> **Note:**
>
> Administrator privileges in Oracle WebCenter Content are required to assign user access to classifications. Your own assigned classification level must also be at least the level being assigned to users. For example, if you are assigned the classification level Secret, you cannot assign the classification level Top Secret to users.

1. Choose **Admin Applets** from the **Administration** menu.
2. Click the **User Admin** icon from the Administration Applets list.
3. On the **Users** tab of the User Admin utility, select the user in the Users list, and click **Edit**.
4. On the Edit User page, make sure the **Info** tab is active.
5. In the **Security Classification** field, select the maximum security level the user should have access to from the option list available on the menu.
6. Click **OK**. Repeat the process for each user.

Note the following considerations:

- If a user is not assigned any security classification, the user cannot pick an initial classification while checking in a content item. Because specifying the initial classification is mandatory, the user cannot check the item into the repository.
- It is recommended that the highest security classification be assigned to the Records Administrator and overall administrator. This allows them to perform all classification-related tasks (for example, on behalf of someone who must downgrade or declassify an item but does not have the required classification privileges).

13.5.2.9 Changing a User's Classification

The assigned security classification of users determines what items they can access.

> **Note:**
>
> Administrator privileges in Oracle WebCenter Content are required to perform this action. Your own assigned classification level must also be at least the level being accessed.

1. Choose **Admin Applets** from the **Administration** menu.
2. Click the **User Admin** icon from the Admin Applets list.
3. On the **Users** tab, select the user in the Users list, and click **Edit**.
4. On the Edit User page, make sure the **Info** tab is active.
5. In the **Security Classification** field, select the new maximum security level the user should have access to. Click the options list arrow, and click the classification needed.

6. Click **OK**.

13.5.2.10 Removing a User's Classification

You may want to remove access from a user who is no longer authorized for a classification or to delete a classification no longer in use. Remove any references to a classification before deletion it.

> **Note:**
>
> Administrator privileges in Oracle WebCenter Content are required to perform this action. Your own assigned classification level must also be at least the level being accessed.

1. Choose **Admin Applets** from the **Administration** menu.
2. Click the **User Admin** icon in the Admin Applets list.
3. On the **Users** tab, select the user in the Users list, and click **Edit**.
4. On the Edit User page, make sure the **Info** tab is active.
5. In the **Security Classification** field, delete the current security level (using the keyboard or by selecting the blank line from list).
6. Click **OK**.

13.5.3 Classification Guides

Classification guides (and their associated topics) enable convenient implementation of multiple classification schemes. They are used to define default values for classification-related metadata fields on the content check-in page such as:

- Initial Classification: (xInitialClassification)
- Reason(s) for classification: (xClassificationReason)
- Declassify exemption category: (xDeclassifyExemptionCategory)
- Declassify on event: (xDeclassifyOnEventDescription)
- Declassify on date: (xDeclassifyOnDate)

Using classification guides makes checking in classified content easier and more consistent, with similar content having the same classification metadata. Classification guides can be further refined by adding topics within a guide.

> **Note:**
>
> Classification guides can be set up only if the ClassifiedEnhancements component is enabled.

13.5.4 Managing Classification Guides

The following tasks are performed when managing classification guides:

- Creating or Editing a Classification Guide
- Deleting a Classification Guide
- Viewing Classification Guide Information
- Creating Classification Topic
- Editing a Classification Topic
- Editing Classification Topic Settings
- Deleting a Classification Topic
- Viewing Classification Topic Information

13.5.4.1 Creating or Editing a Classification Guide

> **Note:**
>
> The Admin.ClassificationGuide right is required to perform this action. This right is assigned by default to the Records Officer and Records Administrator roles.

To create a classification guide:

1. Choose **Records** then **Configure**.
2. Choose **Security** then **Classification Guide**.
3. On the Configure Classification Guide page, click **Add**.
4. On the Create or Edit Classification Guide page, provide a guide ID and a guide name (description), and click **Create**.

   An information page opens showing the identifier and name of the newly created classification guide. The page also includes an **Actions** menu, where current classification guides can be edited or deleted or add topics added to it.
5. Click **OK** to return to the Configure Classification Guide page.

To edit a classification guide:

1. Choose **Records** then **Configure**.
2. Choose **Security** then **Classification Guide**.
3. On the Configure Classification Guide page, select a classification guide to edit from the list and click **Info**.
4. On the information page, choose **Edit** then **Edit Classification Guide** from the page menu.
5. On the Create or Edit Classification Guide page, change the classification guide name as required. The guide ID cannot be modified. Click **Submit Update** when done.

A information page opens showing the identifier and modified name of the classification guide. The page also includes a menu where the current classification guide can be edited or deleted or have topics added to it.

6. Click **OK** to return to the Configure Classification Guide page.

13.5.4.2 Deleting a Classification Guide

> **Note:**
>
> The Admin.ClassificationGuide right is required to perform this action. This right is assigned by default to the Records Officer and Records Administrator roles.

1. Choose **Records** then **Configure**.
2. Choose **Security** then **Classification Guide**.
3. On the Configure Classification Guide page, select the classification guide to delete from the menu and click **Delete**.

   The classification guide is deleted.
4. Click **OK** to return to the Configure Classification Guide page.

13.5.4.3 Viewing Classification Guide Information

> **Note:**
>
> The Admin.ClassificationGuide right is required to perform this action. This right is assigned by default to the Records Officer and Records Administrator roles.

1. Choose **Records** then **Configure**.
2. Choose **Security** then **Classification Guide**.
3. On the Configure Classification Guide page, select the classification guide to view from the menu and click **Info**.

   The Configure Classification Guide page shows the identifier and name of the selected classification guide. The page also includes a menu where the current classification topic can be edited or deleted or have topics added to it.
4. Click **OK** to return to the Configure Classification Guide page.

13.5.4.4 Creating Classification Topic

> **Note:**
>
> The Admin.ClassificationGuide right is required to perform this action. This right is assigned by default to the Records Officer and Records Administrator roles.

To create a classification topic:

1. Choose **Records** then **Configure**.
2. Choose **Security** then **Classification Guide**.
3. On the Configure Classification Guide page, select the classification guide to create the topic for and click **Info**.
4. On the Configure Classification Guide page, choose **Edit** then **Configure Topics** from the page menu.
5. On the Administer Classification Topic page, click **Add**.
6. On the Create or Edit Classification Topic page, provide a name and description for the classification topic, and click **Create** when done.
7. On the Configure Topic Settings page, provide default values for each of the metadata fields, and click **Submit Update** when done.

13.5.4.5 Editing a Classification Topic

To edit a classification topic:

1. Choose **Records** then **Configure**.
2. Choose **Security** then **Classification Guide**.
3. On the Configure Classification Guide page, select the classification guide to edit and click **Info**.
4. From the **Actions** menu on the Classification Guide Information page, choose **Configure Topics**.
5. On the Administer Classification Topic page, select the classification topic to edit from the Topic Name list and click **Info**.
6. Choose **Edit** from the **Actions** menu on the Classification Topic Information page.
7. Edit the description for the classification topic, and click **Submit Update** when done.
8. Click **OK** at the confirmation page to return to the Administer Classification Topic page.

13.5.4.6 Editing Classification Topic Settings

> **Note:**
>
> The Admin.ClassificationGuide right is required to perform this action. This right is assigned by default to the Records Officer and Records Administrator roles.

1. Choose **Records** then **Configure**.
2. Choose **Security** then **Classification Guide**.
3. On the Configure Classification Guide page, select the classification guide to edit and click **Info**.

4. Choose **Configure Topics** from the **Actions** menu on the Information page.
5. On the Administer Classification Topic page, from the Topic Name list, select the classification topic whose settings to edit, and click **Info**.
6. Choose **Edit** then **Edit Topic Settings** from the page menu of the Classification Topic Information page.
7. Modify the default metadata field values as required, and click **Submit Update** when done.

13.5.4.7 Deleting a Classification Topic

> **Note:**
>
> The Admin.ClassificationGuide right is required to perform this action. This right is assigned by default to the Records Officer and Records Administrator roles.

1. Choose **Records** then **Configure**.
2. Choose **Security** then **Classification Guide**.
3. Select the classification guide with a topic to delete on the Configure Classification Guide page and click **Info**.
4. Choose **Configure Topics** from the page menu of the Classification Guide Information page.
5. From the Topic Name list on the Administer Classification Topic page, select the classification topic to delete and click **Delete**.

   A message appears stating the classification topic was successfully deleted.
6. Click **OK** to return to the Administer Classification Topic page.

13.5.4.8 Viewing Classification Topic Information

> **Note:**
>
> The Admin.ClassificationGuide right is required to perform this action. This right is assigned by default to the Records Officer and Records Administrator roles.

1. Choose **Records** then **Configure**.
2. Choose **Security** then **Classification Guide**.
3. Select the classification guide whose topic information is to be viewed on the Configure Classification Guide page and click **Info**.
4. From the page menu on the Classification Guide Information page choose **Edit** then choose **Configure Topics**.
5. From the Topic Name list on the Administer Classification Topic page, select the classification topic to view, and click **Info**.
6. Click **OK** to return to the Administer Classification Topic page.

13.5.5 Supplemental Markings

Supplemental markings can be assigned to content and record folders to clarify document handling in addition to standard document classification. For example, you can add supplemental markings such as Restricted Data or Originator Controlled. Or you can use supplemental markings in collaboration projects. Only people with specific markings will be able to access a group of content. Supplemental markings can be set at both the record folder and the content level.

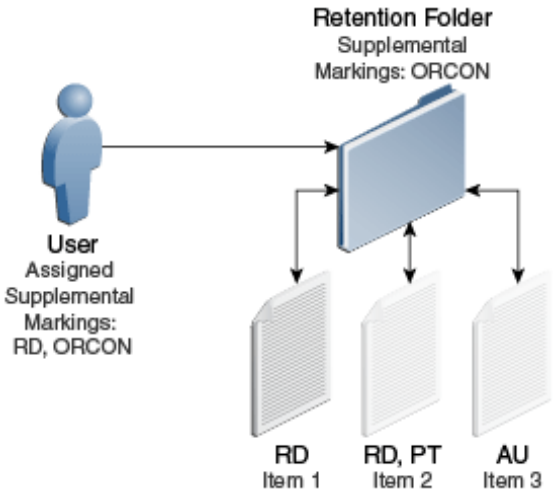
When supplemental markings are assigned to users, even if a user has access to a specific record folder, the supplemental marking further restricts access to record folders and content. In circumstances where a record folder or item has multiple supplemental markings, it can be required that a user match all assigned supplemental markings to access the item. When **Match All** is disabled, if a user matches just one of the multiple supplemental markings, the user can access the object.

To disable use of supplemental markings as a security feature, deselect the **Supplemental Markings** check box on the Configure Retention Settings page and do not assign the markings to users.

Two special supplemental markings, **Restricted** and **Formerly Restricted**, can be used to disable the following classification-related metadata fields on the content check-in and metadata update pages:

- Declassify on event
- Declassify on date
- Downgrade instructions
- Downgrade on event
- Downgrade on date

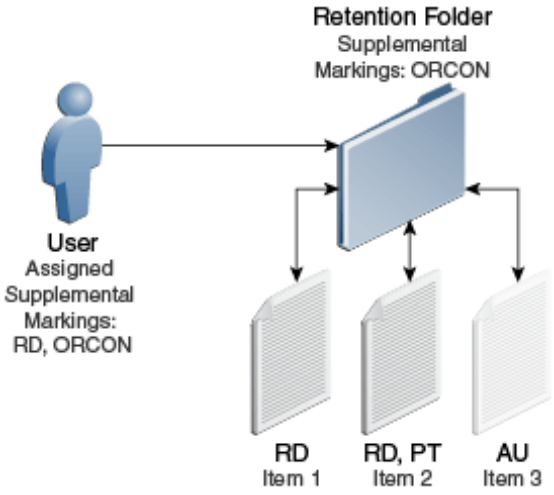
Figure 13-4 User Must Match All Supplemental Markings



For example, in Figure 13-4, the user is assigned the supplemental markings RD and ORCON. The folder is marked with ORCON, therefore the user can access the folder.

The content within the folders are assigned one or more of the markings, RD, PT, and AU. If the security configuration for supplemental markings is set to force the user to match all supplemental markings, then the user can access the folder marked ORCON and its child Item 1 marked with the supplemental marking RD. Because the user has not been assigned the supplemental marking PT or AU, the user cannot access Item 2, which has the multiple markings RD and PT, nor can the user access Item 3 with the marking AU.

Figure 13-5 User Must Match At Least One Supplemental Marking



If the supplemental marking security configuration is not forcing a user to match all markings, then the user can now access Item 2, because the user matches at least one marking RD on the Item 2. Because the user has not been assigned the supplemental marking AU, the user still cannot access Item 3, which has the supplemental marking AU. The user would have to be assigned the supplemental marking AU in the User Admin application to access the item.

Supplemental markings are not inherited by record folders or content. Markings are checked at every folder and item level. Supplemental markings do not have any permissions hierarchy. All markings have equal permissions, either access granted or access denied to users. In contrast, the classified security does have a hierarchy to its classification levels. For further information, see Classified Records Security Hierarchy.

Two special supplemental markings, **Restricted** and **Formerly Restricted**, can be used to disable the following classification-related metadata fields on the content check-in and metadata update pages:

- Declassify on event
- Declassify on date
- Downgrade instructions
- Downgrade on event
- Downgrade on date

To work with supplemental markings, you must have one of the following rights:

- Admin.Triggers: This right enables you to view information about supplemental markings.
- Admin.RecordManager: In addition to viewing information about supplemental markings, this right also enables you to create (add), edit, and delete supplemental markings.

Optionally, the following right may be useful for working with supplemental markings:

- Record.Edit: This right is required to use metadata disabling based on supplemental markings.

> **Note:**
>
> Oracle WebCenter Content administrative permissions are required to perform this action.

13.5.6 Managing Supplemental Markings

The following procedures are followed when managing supplemental markings:

- Enabling or Disabling Supplemental Markings
- Disabling Supplemental Markings
- Creating Supplemental Marking
- Editing a Supplemental Marking
- Viewing Supplemental Marking Information and References
- Deleting a Supplemental Marking
- Assigning User Supplemental Markings
- Removing Supplemental User Markings
- Using Restricted and Formerly Restricted Supplemental Markings

13.5.6.1 Enabling or Disabling Supplemental Markings

You can enable and disable supplemental markings at any time. Enabling supplemental markings enforces the markings assigned to any users attempting to access marked items and record folders.

Disabling supplemental markings means the security provided by the markings is not in force; however, the supplemental markings can still be used generically as document handling instructions.

> **Note:**
>
> The Admin.RecordManager right is required to perform these actions. This right is assigned by default to the Records Administrator role.

To enable supplemental markings:

1. Choose **Records** then **Configure** then **Settings**.
2. In the **Security** section on the Configure Retention Settings page, select **Supplemental Markings**.
3. (Optional) To force a user to match **all** supplemental markings assigned to an item or record folder before granting access, select **User must match all**

Supplemental Markings. To allow access if the user has at least one of the markings, leave the check box unselected.

4. Click **Submit**.

   A confirmation message appears.

13.5.6.2 Disabling Supplemental Markings

To disable supplemental markings:

1. Choose **Records** then **Configure** then **Settings**.
2. In the **Security** section on the Configure Retention Settings page, deselect **Supplemental Markings** and **User must match all supplemental markings**.
3. Click **Submit**.

   A confirmation message appears. Supplemental markings are now disabled and the Supplemental Marking selection field is hidden from view.

13.5.6.3 Creating Supplemental Marking

You can create supplemental markings only if they are enabled. After creating a supplemental marking, it is available to apply to content, record folders, and users.

When editing an existing supplemental marking, its description can be modified but not its name.

> **Note:**
>
> The Admin.RecordManager right is required to perform these actions. This right is assigned by default to the Records Administrator role.

To create a supplement marking:

1. Choose **Records** then **Configure**.
2. Choose **Security** then **Supplemental Markings**.
3. On the Configure Supplemental Markings page, click **Add**.
4. On the Create or Edit Supplemental Marking page, enter a name using a maximum of 30 characters.
5. Enter a description of the marking with a maximum of 30 characters.
6. Click **Create**.

   The Supplemental Marking Information page opens with a message indicating the creation was successful. Use that page to edit or delete the marking, or view references to the marking.
7. Click **OK** when done.

13.5.6.4 Editing a Supplemental Marking

To edit an existing supplemental marking:

1. Choose **Records** then **Configure**.
2. Choose **Security** then **Supplemental Markings**.
3. On the Configure Supplemental Markings page, you can edit the marking in one of two ways:
   - Choose **Edit Marking** from the item's **Actions** menu.
   - Choose the name of the marking to edit. The Supplemental Marking Information page opens. Choose **Edit** from the page menu.
4. On the Create or Edit Supplemental Marking page, make the changes and click **Submit Update.**

   The Supplemental Marking Information page opens with a message indicating the creation was successful. Use this page to edit or delete the marking, or view references to the marking.
5. Click **OK** when done.

13.5.6.5 Viewing Supplemental Marking Information and References

> **Note:**
>
> Either the Admin.Triggers or Admin.RecordManager right is required to perform these actions. The Admin.Triggers right is assigned by default to the Records Officer and Records Administrator roles, and the Admin.RecordManager right to the Records Administrator role.

1. Choose **Records** then **Configure**.
2. Choose **Security** then **Supplemental Markings**.
3. On the Configure Supplemental Markings page, click the name of the marking with information to view.
4. The Supplemental Marking Information page opens. Use the page to edit or delete the marking, or view references to the marking by choosing the appropriate option on the page menu.
5. Click **OK** when done.

13.5.6.6 Deleting a Supplemental Marking

You can delete supplemental markings regardless of whether markings are enabled. A supplemental marking cannot be deleted until all references to the marking in content or record folders is removed. The marking must also be manually removed from any assignments to users.

If a user attempts to delete a supplemental marking currently in use, a message is displayed stating the marking is in use by users (the marking is assigned to users and must be removed), by record folders, or by a content item. The marking must then be removed from the user, folder, or item before proceeding.

To remove the marking from any option lists, the schema must be republished after deleting the marking.

> **Note:**
>
> The Admin.RecordManager right is required to perform this action. This right is assigned by default to the Records Administrator role.

1. Choose **Records** then **Configure**.
2. Choose **Security** then **Supplemental Markings**.
3. On the Configure Supplemental Markings page, choose **Delete** from the item's **Actions** menu. To delete multiple markings, select the check box next to the marking name and choose **Delete** in the **Table** menu. A marking can also be deleted when viewing the marking's Supplemental Marking Information page.
4. A message indicates the deletion was successful.
5. Click **OK**.

> **Note:**
>
> You can search for supplemental markings from the Search page. Select the marking to search for from the Supplemental Markings list on the Search page. Use the search results to see which objects have the marking in use. You can also use screening folders to quickly isolate and sort objects by supplemental markings.

13.5.6.7 Assigning User Supplemental Markings

> **Note:**
>
> Administrator privileges in Oracle WebCenter Content are required to perform this action.

Before assigning markings to users, make sure you have enabled supplemental markings, created the markings, assigned supplemental markings to record folders and retained content, and assigned roles to the users. For the most strict supplemental marking security, you can also force a user to pass all supplemental markings to access an item or record folder.

You may want to remove access from a user who is no longer authorized for a supplemental marking, or to delete a supplemental marking no longer in use. You must remove any references to a supplemental marking before you can delete it.

To disable use of supplemental markings as a security feature, do not assign the markings to users.

To assign a supplemental marking to a user:

1. Choose **Admin Applets** from the **Administration** menu.
2. Click the **User Admin** icon from the list of Admin Applets.

3. On the **Users** tab, select the user in the Users list, and click **Edit**.

   The **Info** tab on the Edit User page opens.

4. In the **Supplemental Markings** field, select the markings to which the user should have access. Click the options list arrow, and highlight the marking. Multiple markings can be assigned to a user.
5. Click **OK**. Repeat the process for each user who needs markings.
6. Restart Content Server.

13.5.6.8 Removing Supplemental User Markings

To remove a supplemental marking from a user:

1. Choose **Admin Applets** from the **Administration** menu.
2. Click the **User Admin** icon in the list of Admin Applets.
3. On the **Users** tab, select the user in the Users list, and click **Edit**.

   The **Info** tab on the Edit User page opens.

4. In the **Supplemental Markings** field, delete a marking by editing the text in the **Supplemental Markings** field.

   > **Caution:**
   >
   > Be careful when editing text in this field. Each supplemental marking must have a comma and a space between markings, or an access denied error occurs when trying to access content with multiple markings and **Match All Markings** is enabled.

5. Click **OK**. Repeat for each user who has a marking to be removed.
6. Restart Content Server. For more information about restarting, see *Administering Oracle WebCenter Content*.

13.5.6.9 Using Restricted and Formerly Restricted Supplemental Markings

Restricted Data and *Formerly Restricted Data* are supplemental markings shipped with the product. Those markings can be used alone or in combination with other markings to disable classified metadata fields on the content check-in and metadata update forms:

1. Enable supplemental markings.
2. Click **Restricted Data** or **Formerly Restricted Data** as the supplemental marking.
3. Restart Content Server.

13.6 Custom Security

Custom security is optional and are another layer of security in addition to supplemental markings.

Two types of custom security are available:

- Simple custom security fields, where custom field are configured to be matched by a user rather than a designated supplemental marking. This is called *custom supplemental markings* in the DoD 5015 standard,
- Advanced custom security, where security is applied to fields that use option lists. Security can be applied to individual items in the option list.

Unlike supplemental markings, custom security is enforced at the item level. Supplemental markings are enforced at both the record folder and the item level.

To work with custom security, you need to have one of the following rights:

- Admin.Triggers: This right enables you to view information.
- Admin.RecordManager: In addition to viewing information, this right also enables you to create (add), edit, and delete custom security.

A *simple custom security field* pairs a custom content field with a custom user field. For example, you can create a custom security field such as Project Name. Users must be assigned the appropriate project name or names to access or view an item assigned with custom security. If the Match All setting is enabled, a user must be assigned to all the same projects as an item is assigned to for the user to access an item with multiple project assignments. If a user does not match all project names, the user cannot access an item.

You can opt to select the match all feature for custom security fields just as you can with supplemental markings. Content is then checked in with one or more custom security field options, such as a particular project name, assigned to the content.

For instance, User1 is assigned project name Pangea only. The user named User2 is assigned both project name Pangea and Tectonic. If content is checked in with multiple field options assigned (for example, Pangea and Tectonic), then only a user with all project names assigned (User2) can access that content. If the Match All setting is disabled, then a user only must match one field option to access an item.

Advanced custom security also limits access to content items. Advanced security can also restrict access based on aliases as well as individual users. This type of security assigns security at the *item* level for option lists. When using this type of security, the only metadata that can be used is that which has an option list associated with it. Access can then be restricted to individual items in the option list by limiting which accounts, which users, or which aliases of users can access specific options.

This section covers the following topics:

- Managing Custom Security
- Simple Custom Security Field Example

13.6.1 Managing Custom Security

The following tasks are often performed when managing custom security:

- Enabling or Disabling Custom Security Usage
- Creating a Simple Custom Security Field
- Editing a Custom Security Field
- Adding Advanced Security
- Editing Advanced Security
- Viewing Simple Custom Security Field Information

- Deleting a Simple Custom Security Field (Simple)

13.6.1.1 Enabling or Disabling Custom Security Usage

Use this procedure to enable the custom security feature. It can be enabled or disabled at any time.

> **Note:**
>
> The Admin.RecordManager right is required to enable custom security. This right is assigned by default to the Records Administrator role.

1. Choose **Records** then **Configure** then **Settings**.
2. On the Configure Retention Settings page, expand the **Security** section if needed. Select **Custom Security**.
3. Click **Submit Update**.

   A message appears indicating the configuration was successful.
4. Click **OK**.

To disable the feature, deselect **Custom Security**.

13.6.1.2 Creating a Simple Custom Security Field

Use this procedure to create a new simple custom security field.

> **Note:**
>
> Make sure you have defined the custom field for the items in the Configuration Manager utility, and the custom field for the users in the User Admin utility before performing this task.

You can create custom security fields only if the custom security field feature has been enabled.

> **Note:**
>
> The Admin.RecordManager right is required to perform this action. This right is assigned by default to the predefined Records Administrator role.

To create a custom security field:

1. Choose **Records** then **Configure**.
2. Choose **Security** then **Custom Security**.

3. Click **Add** in the Custom Security Field area on the Configure Custom Security page.
4. Enter a name for the field on the Create or Edit Simple Custom Security Field page.
5. Select the document metadata name for the content field from the **Content Field** list.
6. Select the metadata name of the user field from the **User Field** list.
7. (Optional) Select **Match all** to force the user entries to match **all** content field entries. Leave this box unselected to allow only one content field to match the user field.
8. Click **Create**.

   A message appears indicating success.
9. Click **OK**.

13.6.1.3 Editing a Custom Security Field

To edit an existing custom security field:

1. Choose **Records** then **Configure**.
2. Choose **Security** then **Custom Security**.
3. Choose **Edit Field** from a field's **Actions** menu on the Configure Custom Security page.
4. Make the necessary edits:
   a. Select the name of the metadata field from the **Content Field** list.
   b. Select the name of the user metadata field in the **User Field** list.
   c. Select (if needed) **Match all**.
5. Click **Submit Update**.

   A message states the update was successful.
6. Click **OK**.

13.6.1.4 Adding Advanced Security

Use this procedure to add advanced security to an existing field. The field used must be one that has an option list associated with it. The option list must be created before this feature can be used.

You can add custom security only if the custom security feature is enabled.

> **Note:**
>
> The Admin.RecordManager right is required to perform this action. This right is assigned by default to the predefined Records Administrator role.

To add advanced security to an existing custom security field:

1. Choose **Records** then **Configure**.
2. Choose **Security** then **Custom Security**.
3. If needed, click the **Advanced Custom Security** tab on the Configure Custom Security page to open that page. Click **Add**.

4. In the Select Security dialog, select a field from the list. Note that only fields with option lists are available for selection.
5. Click **OK**.
6. On the Advanced Custom Security Option page, choose the **Actions** menu for the option item that needs security. Click **Edit Security**.
7. In the Select Security dialog, select users or aliases who will have access to content items with that individual option list value.
8. If needed, select a security group from the list.
9. The Advanced Custom Security Option page opens, showing the selections just made.

13.6.1.5 Editing Advanced Security

To alter custom security for a field (including removing the security):

1. Choose **Records** then **Configure**.
2. Choose **Security** then **Custom Security**.
3. In the **Advanced Custom Security** area of the Configure Custom Security page, choose **Edit Security** from the **Actions** menu of the option item. To remove security for the option item, choose **Remove Security** from the **Actions** menu of the option item.

   When editing, a dialog opens so you can select a field for use. Only fields with option lists are available for selection.
4. Click **OK**.
5. On the Advanced Custom Security Option page, choose **Edit Security** from the **Actions** menu for the option item that needs security.
6. In the Select Security dialog, select users or aliases who will have access to content items with that individual option list value.
7. If needed, select a security group from the list.
8. The Advanced Custom Security Option page opens, showing the selections just made. The security is now in place.

13.6.1.6 Viewing Simple Custom Security Field Information

> **Note:**
>
> Either the Admin.Triggers or Admin.RecordManager right is required to perform this action. The Admin.Triggers right is assigned by default to the Records Officer and Records Administrator roles, and the Admin.RecordManager right to the Records Administrator role.

1. Choose **Records** then **Configure**.
2. Choose **Security** then **Custom Security**.

3. In the custom field area on the Configure Custom Security page, click the field to view.

   The Information page opens.

4. Click **OK** when done.

13.6.1.7 Deleting a Simple Custom Security Field (Simple)

You can delete a custom security field without having to remove references to it by users and content, unlike supplemental markings and security classifications.

> **Note:**
>
> The Admin.RecordManager right is required to delete a custom security field. This right is assigned by default to the Records Administrator role.

1. Choose **Records** then **Configure**.
2. Choose **Security** then **Custom Security**.
3. On the Configure Custom Security page, choose **Delete** from the item's **Actions** menu. To delete multiple fields, select the check box next to the field name and choose **Delete** in the **Table** menu. A field can also be deleted when viewing the field's Information page.
4. A message appears, stating the deletion was successful.
5. Click **OK**.

13.6.2 Simple Custom Security Field Example

This example gives step-by-step instructions for setting up a custom security field called Project Name. It includes the following processes:

1. Create the Custom Security Field in Configuration Manager.
2. Create the Custom Security Field in User Admin. Oracle WebCenter Content assigns the u prefix. Assign the field options to the user.
3. Rebuild the search index, and restart Content Server.
4. Create the Custom Security Field using the exact field names defined in the Oracle WebCenter Content utilities.

After the custom security field is set up, test the field by checking in and accessing items assigned field options. See Verify the Custom Security Field.

13.6.2.1 Create the Custom Security Field in Configuration Manager

This portion of the example creates the custom security field as a document field within the Configuration Manager utility. The field will be available for use on the check-in form.

1. Choose **Admin Applets** from the **Administration** menu.
2. Click the **Configuration Manager** icon in the Admin Applets list.
3. Click the **Information Fields** tab in the Configuration Manager utility.
4. Click **Add**.

5. On the Add Custom Info Field page, type **`ProjectName`**, and click **OK**. On the Add Custom Info Field page, specify the field attributes:
    a. For **Field Caption**, enter a space between any compound words (in the above example, Project and Name) so the field label displays properly.
    b. In the **Field Type** list, select **Long Text**.
    c. Select **Enable Options List**. Click the enabled **Configure** button.

       The Configure Option List page opens.
    d. In the **Options List Type**, select the **Edit and Multiselect List** option.
    e. Click **Edit** next to **Use Option List**.

       The Option List page opens.
    f. In the options list, type **`Pangea`**. Press Enter for a carriage return, then type **`Tectonic`**.
    g. Click **OK** three times.
6. Click **Update Database Design**.

13.6.2.2 Create the Custom Security Field in User Admin

This portion of the example creates the custom security field as an information field called Project Name within the User Admin utility.

1. Choose **Admin Applets** from the **Administration** menu.
2. Click the **User Admin** icon in the Admin Applets list.
3. On the User Admin utility, open the **Information Fields** tab.
4. Click **Add**.
5. On the Add Custom Info Field page, type **`ProjectName`** and click **OK**. Specify the field attributes on the Add Metadata Field page:
    a. For **Field Caption**, enter a space between any compound words (as in the example, Project and Name) so the field label displays properly.
    b. In the **Field Type** list, select **Long Text**.
    c. Select **Enable Options List**. This enables the **Options List Settings** tab.
    d. In the **Options List Type**, click the **Edit and Multiselect List** option.
    e. Choose **Edit**.
    f. In the options list, type **`Pangea`**. Press Enter for a carriage return, and then type **`Tectonic`**.
    g. Click **OK** twice.
6. Click **Update Database Design**.
7. Click the **Users** tab. Create a user named `User1` then select that name and click **Edit**. The Edit User page for the user opens.
    a. In the Project Name list, click the down arrow, and select the project name Pangea from the list. Repeat for Tectonic. You now have a comma-separated list of project names assigned to User1.
    b. Click **OK**.

8. Restart Content Server.

13.6.2.3 Create the Custom Security Field

This portion of the example creates the custom security field. Make sure the Custom Security Field option is enabled in the Configure Retention Settings page, and you have defined the document and user fields in the appropriate administration utilities.

1. Click **Configure** then **Custom Security Fields** from the Configure Retention Settings page.
2. On the Configure Custom Security page, click **Add**.
3. In the Custom Security Field on the Create or Edit Simple Custom Security Field page, type **`Project Name`**.
4. From the **Content Field** list, select **ProjectName**.
5. From the **User Field** list, select **ProjectName**.
6. Select **Match all** to force a user to match all content field entries. This is the strictest setting. If a user is not assigned all project names assigned to an item, the user cannot access that item.
7. Click **Create**.

13.6.2.4 Verify the Custom Security Field

This portion of the example demonstrates how the custom security field restricts access.

- Log in as User1 and check in an item with both Pangea and Tectonic selected as project names in the check-in form. Search for the item you just checked in as User1. The search should be successful.
- Now log in as a new user without any custom field assignments. Attempt to access the item user1 just checked in. The attempt to view the item should not be successful because the new user does not have any assigned field options.
- Log in as an administrator and assign the new user the field option Pangea. Disable the **Match all** option for the custom security field. Log in as the new user and attempt to access the item with Pangea and Tectonic assigned as the project name. The access should now be successful because only one field list option has to match, and the user is assigned the appropriate field list option.

14

Defining and Processing Dispositions

This chapter discusses setting up and administering disposition scheduling in Oracle WebCenter Content: Records. It provides information on setting up triggers, which can start a disposition, setting up freezes, which can halt a disposition, as well as processing of disposition actions. Dispositions are the actions taken on content, usually for items no longer required for conducting current business. The following topics are covered:

- Working with Triggers
- Managing Freezes
- Creating Dispositions
- Processing Dispositions

14.1 Working with Triggers

A trigger starts the processing of a disposition instruction upon the occurrence of a triggering event. Triggers are associated with a disposition rule for a retention category. A triggering event can be a change in content item state, completed processing of a preceding disposition action, retention period cutoff, and custom triggers.

Two types of triggers are provided to initiate disposition processing. System derived triggers are built-in triggers based on defined events. Custom triggers can be created by administrators to define specific events.

To work with triggers, the following rights are required:

- Admin.RecordManager: This right enables a user to view information about triggers.
- Admin.Triggers: In addition to viewing information about triggers, this right also enables a user to create (add), edit, and delete triggers.

Security groups can be used to block access to triggers. For example, if you do not want users with the Admin.Triggers right to be able to edit and delete triggers, you can use security groups to restrict access to these functions. Only users with access privileges to the security group assigned to a trigger can edit and delete the trigger.

This section discusses the following topics:

- System-Derived Triggering
- Types of Triggers
- Trigger Management
- Trigger Examples

14.1.1 System-Derived Triggering

System-derived triggering uses the following built-in events:

- Retention Period Cutoff

- Preceding (Disposition) Action
- Content or Folder States

14.1.1.1 Retention Period Cutoff

Retention period cutoff causes a cutoff action to occur at the end of the time unit specified in the retention period. After cutoff, the content item is retained for the retention period specified in the disposition rule. For instance, when retention period cutoff is used as a triggering event and a retention period of three calendar years is specified, the cutoff takes place at the end of the current year and the affected content is retained for three years after the end-of-year cutoff.

Trigger retention periods are available if the `AllowRetentionPeriodWithCutoff` variable is enabled. It is enabled by default.

Note that negative retention periods are available only if the following variables are enabled in the `records_management_environments.cfg` file:

- `AllowRetentionPeriodWithoutCutoff=1`. When enabled, retention periods are allowed with other triggering events in addition to the default ones of Cutoff and Preceding Action.

  ```
  dDispPeriod:allowSignedInteger=1
  dDerivedMonthDelay:allowSignedInteger=1
  dDerivedDayDelay:allowSignedInteger=1
  ```

- When enabled, a negative retention period can be supplied for any trigger *except for* Cutoff and Preceding Action.

  For example:

  ```
  Triggering Event =Contract Ended
  Retention Period =-1 month
  Disposition Action =Notify Authors
  Triggering Event =Preceding Action
  Retention Period =3 months
  Disposition Action =Archive
  ```

14.1.1.2 Preceding (Disposition) Action

When a preceding action in a disposition instruction sequence completes processing, the next subsequent rule begins. The system tracks when a preceding action completes, and automatically triggers the next step in a disposition sequence.

14.1.1.3 Content or Folder States

System-derived global triggers based on an item or folder state can be affected by an implicit or explicit change in an item or a record folder. An example of an implicit change is when an item has an activation date set in the future. The system is aware of the future activation date and it activates the item at the indicated date and automatically changes the state of the item to active. The Records Administrator does not have to perform any explicit action other than indicating the future activation date. An example of an explicit change in state is when an administrator manually cancels or expires a specific item. When content assumes another trigger-dependent state, the associated disposition rule operates on the item.

14.1.2 Types of Triggers

Custom triggers are explicitly defined by an administrator. Custom triggers are more inclusive and less granular than a system-derived trigger based on content state. A system-derived trigger may only affect one content item within a retention category, because it may be the only item in a given state but a custom trigger can affect all eligible content within a given retention category.

Three types of custom triggers can be defined:

- Global triggers, which happen at a time defined by an administrator.
- Custom direct triggers, which use metadata fields as triggering events.
- Custom indirect triggers, which occur on a regular schedule based on audit events.

The triggers appear in the Triggering Events list of the Disposition Rules page.

Access to creating, editing, and viewing information about triggers can be controlled by security settings. If ACL security is enabled, access to triggers by group and user permissions can be restricted. If default security is used, then the trigger can be assigned to a security group and the filer be designated.

> **Note:**
>
> The metadata fields `dReleaseDate` and `dCreateDate` cannot be used as trigger dates, because the indexer process that populates them cannot trigger a re-computing of the lifecycle.

Global triggers have an activation date. The activation date can be a past, present, or future date. A user can create a trigger and delay the activation of a trigger for an indefinite amount of time until activation is required. In essence this is a dormant trigger, which does not contain an activation date.

A user can create a trigger that activates immediately, activate a trigger on a certain date and time, or delay the activation of a trigger for an indefinite amount of time until activation is required.

Custom direct triggers are used to create customized trigger functionality in addition to the global triggers built into the product and operating behind the scenes. Custom direct triggers are system-derived triggers based on a content state, on content, or record folder date fields only. These triggers are not global triggers. They only affect an item meeting a given state. Unlike regular (global) or event (indirect) triggers, an activation date is not set explicitly for the custom direct trigger and it is not enabled. When created, the custom direct trigger is always active and ready to be used.

Custom direct triggers can be created with a date field, folder date field, or both. There is no logical AND relationship between the content and folder date fields. There is a logical AND relationship between content fields or between folder fields if more than one field is specified. The fields are used to activate the trigger for content and the folder fields are used to activate the trigger for folders.

Unlike a regular (global) trigger, an *indirect trigger* has a life cycle. Audit Approval is the built-in indirect trigger. This trigger is based on an audit event. It requires that **Subject to Audit** be

selected when checking in a content item, and an audit period selected from the Audit list on the check-in page.

The indirect trigger feature saves time in setting up and maintaining triggers that repeat on a regular basis. The Records Administrator must populate the annual triggers list.

14.1.3 Trigger Management

Several tasks are involved in managing triggers, as discussed in the following sections:

- Creating a Trigger
- Editing a Trigger
- Viewing Trigger Information
- Viewing Trigger References
- Deleting a Trigger
- Setting Up Indirect Triggers
- Deleting an Indirect Trigger Date Entry
- Disabling an Indirect Trigger Period

14.1.3.1 Creating a Trigger

> **Note:**
>
> The Admin.Triggers right is required to perform this action. This right is assigned by default to the Records Administrator and Records Officer roles.

To assign more granular security settings on triggers than the default roles, be sure that ACL security settings are enabled and users are assigned to roles and to an alias for any group permissions.

When creating an indirect trigger, the content field on which the indirect trigger is based must already be created in the Configuration Manager utility. In addition, the period option list for the indirect trigger periods must be populated.

Custom triggers are not usually created using a PCM field for the trigger. To use a PCM field for a trigger, you must first create a field to be used. The field must be prefixed with an x (for example, `xPhysicalDateField`). A similar field must be created in the Configuration Manager with the same name, with no prefix (for example, `PhysicalDateField`). After the fields are created, the field can be selected for use with the trigger.

For details about creating a custom field, see Creating a Simple Custom Security Field.

To create a trigger:

1. Choose **Records** then **Configure** from the top menu.
2. Choose **Retention** then **Triggers** from the page menu.

3. On the Configure Triggers page, select the type of trigger to create (Global, Custom Direct, or Indirect). Choose **Add**.
4. On the Create or Edit Trigger Type page, select a **Security Group** and **Author** from the lists if default security is enabled. Otherwise, the default Security Group is always RecordsGroup and the author defaults to the user with the Records Administrator or Records Officer role who created the trigger, even if these fields are not displayed at the time the trigger was created.
5. (Optional) If the organization uses the accounts security model, indicate the **Account** for the trigger.
6. Enter a name to a maximum of 100 characters.
7. Enter specific Trigger Information:

   Global Triggers Only: Enter an Activation Date. If not entered it is considered a dormant trigger, which can be activated later.

   Custom Direct Triggers only: Optional, but at least one Content or Folder Date Field should be selected. Select a **Content Date** field or fields for the trigger from the **Content Date Field(s)** list. The field is subject to an ACL character limitation of 100 characters, although the database can be changed to accept more characters into this field.

   Custom Indirect Trigger: Select a content field on which the indirect trigger is based and a folders field on which the indirect trigger is based.

   The **New Revision Date** option is available only if **Enable New Revision Date Trigger Field** was selected during configuration. With this date field selected, whenever a new revision of a content item is checked in, all revisions of the content item, including the latest one, are stamped with the date of the new revision. With this functionality retention rules such as *Delete if not updated in X number of years* can be created.
8. **Synchronize on Period Start Date**: If selected, the start date is used to synchronize the trigger. This is similar to a cutoff disposition action. For example: if a disposition is *After activate wait 1 month then delete*, if a record is activated on 1/15/10, then the system will synchronize to 1/31/10 and add 1 month before deleting.
9. (Optional) If ACL-based security is enabled, click **Group** and **User Permissions** for the trigger. This limits who can edit the trigger.
10. Click **Create**.

    A message appears stating the trigger was created successfully.
11. Click **OK**.

    Custom Indirect Triggers: Enter the date periods for the trigger.

14.1.3.2 Editing a Trigger

To modify an existing trigger:

1. Choose **Records** then **Configure** from the top menu.
2. Choose **Retention** then **Triggers** from the page menu.
3. On the Configure Triggers page, select the type of trigger to edit (**Global**, **Custom Direct**, or **Indirect**).
4. Choose **Edit** then **Edit Trigger** from the item's **Actions** menu for the trigger to edit.
5. On the Create or Edit Trigger Type page, make the changes to the applicable fields.
6. Click **Submit Update**.

A message appears stating the trigger was updated successfully.

7. Click **OK**.

14.1.3.3 Viewing Trigger Information

> **Note:**
>
> Either the Admin.Triggers or Admin.RecordManager right is required to perform this action. The Admin.Triggers right is assigned by default to the Records Administrator and Records Officer role, and the Admin.RecordManager right to the Records Administrator role.

To view trigger information:

1. Choose **Records** then **Configure** from the top menu.
2. Choose **Retention** then **Triggers** from the page menu.
3. On the Configure Triggers page, select the type of trigger to view (**Global**, **Custom Direct**, or **Indirect**).
4. Click the trigger name to view.
5. When done, click **OK**.

14.1.3.4 Viewing Trigger References

> **Note:**
>
> Either the Admin.Triggers or Admin.RecordManager right is required to view references to a trigger. The Admin.Triggers right is assigned by default to the Records Administrator and Records Officer role, and the Admin.RecordManager right to the Records Administrator role.

To view references to a trigger (those disposition rules using the trigger in their definitions):

1. Choose **Records** then **Configure** from the top menu.
2. Choose **Retention** then **Triggers** from the page menu.
3. On the Configure Triggers page, select the type of trigger to view (**Global**, **Custom Direct**, or **Indirect**).
4. Click the trigger name to view.
5. On the page menu on the Trigger Information page, choose **References**.

   The Trigger References page opens, showing category dispositions the current trigger is referenced by, with a link to each of the referencing category disposition. If the link is clicked, the Disposition Information page of the referencing disposition opens.
6. When done, click **OK**.

14.1.3.5 Deleting a Trigger

> **Note:**
>
> The Admin.Triggers right is required to perform this action. This right is assigned by default to the Records Administrator and Records Officer role. In addition, you must have delete permission (D) for the trigger's security group. The Records Officer roles does not have this permission by default.

If a trigger is in use, all references to the trigger must be removed before it can be deleted. Triggers are referenced by triggering events in disposition rules.

To delete a trigger:

1. Choose **Records** then **Configure** from the top menu.
2. Choose **Retention** then **Triggers** from the page menu.
3. On the Configure Triggers page, select the type of trigger to view (**Global**, **Custom Direct**, or **Indirect**). Navigate to the trigger to delete.
4. Choose **Delete Trigger** on the trigger's **Actions** menu.

   A message appears stating the trigger was deleted successfully.
5. Click **OK**.

To delete multiple triggers, select the trigger check boxes and choose **Delete** from the table menu.

14.1.3.6 Setting Up Indirect Triggers

> **Note:**
>
> The Admin.Triggers right is required to perform this action. This right is assigned by default to the Records Officer and Records Administrator roles.

The Audit Approval indirect trigger is the only built-in indirect trigger available. Use the same procedure for any other indirect triggers to be created. Select the trigger name and follow the same steps to populate those triggers.

To specify the dates required:

1. Choose **Records** then **Configure** from the top menu.
2. Choose **Retention** then **Triggers** from the page menu.
3. On the Configure Triggers page, click the **Indirect** tab. Choose **Trigger Dates Info** from the **Actions** menu for the Audit Approval trigger.
4. Choose **Trigger Dates Info** on the page menu.
5. On the Indirect Trigger Date Entries page, click **Add**.

6. On the Create or Edit Indirect Trigger Date Entries page, select the trigger period that needs an activation date. If the defaults will not be used, populate the Trigger Period list in the Configuration Manager utility before performing this action.
7. Enter an activation date for the trigger period. Select the date from the Calendar icon. The time can be edited directly in the Activation Date text box. Be sure to use the time format configured by the system defaults.
8. Click **Create**.

   The Trigger Date Entry information is added to the Indirect Trigger Date Entries for Audit Approval page.
9. Repeat as needed to define dates for each indirect trigger period.

14.1.3.7 Deleting an Indirect Trigger Date Entry

> **Note:**
>
> The Admin.Triggers right is required to perform this action. This right is assigned by default to the Records Administrator and Records Officer roles.

To delete a date entry (trigger period) for an indirect trigger:

1. Choose **Records** then **Configure** from the top menu.
2. Choose **Retention** then **Triggers** from the page menu.
3. Choose **Delete** from the trigger's **Actions** menu on the Configure Triggers page.

14.1.3.8 Disabling an Indirect Trigger Period

> **Note:**
>
> The Admin.Triggers right is required to perform this action. This right is assigned by default to the Records Administrator and Records Officer roles.

Disabling an indirect trigger period inactivates the trigger, but retains the trigger for archival purposes. The trigger period can be disabled for both built-in and custom indirect triggers.

To disable an indirect trigger period at the date entry level:

1. Choose **Records** then **Configure** from the top menu.
2. Choose **Retention** then **Triggers** from the page menu.
3. On the Configure Triggers page, choose **Edit** then **Edit Trigger** from the trigger's **Actions** menu.
4. On the Create or Edit Trigger Type page, select the trigger period to disable from the trigger period list, and click **Info**.
5. On the Create or Edit Indirect Trigger Date Entries page, deselect **Enabled**, and click **Submit Update**.

The Enabled field for the Trigger Period that was edited now displays `No`.

6. Click the **Configure Retention Schedule Components** link at the top of the page to return to the Configure Retention Schedule Components page.

14.1.4 Trigger Examples

This section provides examples of the following triggers:

- Global Triggers
- Custom Direct Trigger

14.1.4.1 Global Triggers

This example creates a global trigger. An active trigger is one that is activated and enabled immediately with no delay in the activation date. In this example, an event trigger with a known activation date is created.

1. Choose **Records** then **Configure** then **Triggers**.
2. On the Configure Triggers page, click **Add** in the Global Trigger area.
3. Enter `Case 123 Closed` as the name on the Create or Edit Trigger Type page.
4. Enter an **Activation Date**, either the current date or an earlier date. The activation time is midnight (12:00 AM) by default.
5. Click **Create**.

   A message appears stating the trigger was created successfully. The **Enabled** label indicates `Yes` and the **Activation Date** is displayed.

Global triggers can be created with a future activation date. The activation of the trigger is delayed until the date and time specified. A user can backdate trigger activation. To do so, use a future activation date when creating the global trigger.

Triggers can be created with an activation date that is delayed until an activation date is entered. This is a dormant, inactive trigger. A dormant trigger is useful for event triggers when it is known that an event is going to occur, but the exact date is unknown. To avoid system processing overhead, do not enable the trigger.

To create a dormant global trigger, do not enter an activation date when creating the trigger, but enter it at a later time.

A disabled, dormant trigger can be activated without an activation date set for the future. To do so, edit the trigger and enter the activation date.

14.1.4.2 Custom Direct Trigger

This example creates a custom direct trigger for a custom field based on the termination date of an employee. After the employee termination date is entered on the Content Info Update form, the direct triggers and the item begins its disposition processing.

1. Create the custom field for the Employee Termination Date using the Configuration Manager utility.
2. Create a custom direct trigger keyed off a date field.

3. Set up the disposition instruction activated by this custom trigger. The disposition instruction performs the cutoff when the employee termination date is entered, retains the item for 3 years, and then destroys the record.
4. As a last step, test the trigger to verify it is working correctly.

14.1.4.2.1 Creating a custom field

Create the custom field for the Employee Termination Date using the Configuration Manager utility.

1. Choose **Admin Applets** from the **Administration** menu.
2. Choose **Configuration Manager** from the list of Admin Applets.
3. In the Configuration Manager utility, click the **Information Fields** tab and click **Add**.
4. On the Add Custom Info Field page, enter **`EETermDate`** as the Field Name and click **OK**.
5. On the Edit page, enter **`Employee Termination Date`** as the Field Caption.
6. In the **Field Type** list, select **Date**.
7. Verify that **Required** is not selected and **User Interface** and **Search Index** are selected (typical defaults).
8. Click **OK**.
9. Click **Update Database Design**.

14.1.4.2.2 Creating a custom direct trigger

Create a custom direct trigger keyed off a date field.

1. Choose **Records** then **Configure** then **Triggers** from the top menu.
2. On the Configure Triggers page, click **Add** in the Custom Trigger area.
3. On the Create or Edit Trigger Type page, enter **`EE Term Date`** as the Trigger Name.
4. Enter **`Employee Termination Date`** as the Brief Description.
5. In the **Content Date Field(s)** list, click **EETermDate**.

   The field is populated with `xEETermDate`.
6. Click **Create**.

   A message appears stating the custom direct trigger was created successfully.

14.1.4.2.3 Setting up the disposition instruction

Set up the disposition instruction activated by this custom trigger. The disposition instruction performs the cutoff when the employee termination date is entered, retains the item for 3 years, and then destroys the record. This example creates disposition rules for a category named Employees. To create the category and disposition instruction:

1. Choose **Browse Content** then **Retention Schedules**.

2. On the Exploring Retention Schedule page, choose **Create** then **Create Retention Category** on the page menu.
3. On the Create or Edit Retention Category page, enter **`EE-RC-1`** as the Retention Category Identifier.
4. Enter **`Employees`** as the Retention Category Name.
5. Enter **`Employee Retention Category`** as the Retention Category Description.
6. (Required for U.S. Government Agencies) Enter **`EE-RC-1`** as the code of the authority for the disposition.
7. Click **Create**. On the Disposition Instructions page, create the first rule:
   a. Click **Add**.
   b. On the Disposition Rule page, select the new custom direct trigger called EE Term Date in the **Triggering Event** list.
   c. In the **Disposition Action** list, select **Cutoff**.
   d. Click **OK**.
8. Create the second rule:
   a. Click **Add**.
   b. On the IDisposition Rule page, select Preceding Action in the **Triggering Event** list.
   c. In the Retention Period field, enter **3** and click **Calendar Years**.
   d. In the **Disposition Action** list, select **Destroy**.
   e. Click **OK**.
   f. Click **Submit Update**.

      A message appears with a summary of the disposition.
9. Click **OK**.

To test the trigger enter an expiration date for a test employee content item in the Info Update Form, accessed with the **Update** option in the **Actions** menu of the content information page. The content item begins disposition processing on the cutoff date. If you check the life cycle for the content item, you can see the dates are already set for the processing.

14.2 Managing Freezes

A freeze (sometimes called a *dynamic hold*) inhibits disposition processing for an item. This can be used to comply with legal or audit requirements, such as when a legal hold must be placed on information. Different types of freezes can be defined to refine the freeze/hold process needed in an organization.

For information about using Federated Freeze during legal processing, see Using Federated Search and Freeze.

> **Note:**
>
> Creating custom disposition actions requires in-depth technical knowledge of Oracle WebCenter Content. To define custom disposition actions, contact Consulting Services.

If an item is frozen, all revisions of the item are frozen. The frozen revision is frozen directly and the other revisions inherit the freeze. Recurring freezes can also be scheduled for selected items of content.

The following tasks are involved in managing freezes:

- Creating a Freeze
- Editing a Freeze
- Viewing Freeze Information
- Deleting a Freeze
- Freezing Items, Folios or Folders
- Unfreezing Frozen Items or Folders
- Searching for Frozen Content and Folders
- Re-Sending an Email Notification for a Freeze
- Example: Creating a Freeze

14.2.1 Creating a Freeze

> **Note:**
>
> The Admin.RecordManager right is required to perform this action. This right is assigned by default to the Records Administrator role.

To create a freeze:

1. Choose **Records** then **Configure** from the top menu.
2. Choose **Retention** then **Freezes**.
3. Click **Add** on the Freeze Configuration page.
4. On the Create or Edit Freeze page, select a Security Group from the list. This field is only displayed if default security is enabled on the Configure Retention Settings page.
5. In the **Filer** field, specify the person who is responsible for creating the freeze. This will normally be the person currently logged in, so the default does not generally need to be changed, but a different user can be chosen from the list if required.
6. Specify a name for the freeze.
7. (Optional) Specify a description for the freeze.
8. (Optional) Specify group and user permissions to restrict who has access to the freeze. These fields are only displayed if ACL-based security is enabled on the Configure Retention Settings page.
9. (Optional) Specify the end date of the freeze.

> **Note:**
>
> The items are not unfrozen automatically at the specified date. This must be done manually. This field is used for tracking and documentation purposes only.

10. (Optional) Specify a descriptive text with instructions for unfreezing the items.
11. (Optional) Specify if a notification should be sent about the freeze. Notifications are first sent out when the freeze is created.
12. Enter the email address of people to receive the freeze notification and the email address of the person initiating the email. If left blank, the send of the notification is the user who created the freeze.

    For example, you could create a freeze for a lawsuit and notify all people working on the lawsuit they need to check in any items pertaining to the lawsuit using the associated freeze.

    Use commas to separate multiple email addresses. Spaces are ignored. Do not press Enter to put email addresses on separate lines. If you do, all e-mail addresses after the first line break will not receive the notification.

    Required if **Send Notification** is selected. Maximum characters: 3,000.

    The email is (re)sent when **Create** (on the Create Freeze page) or **Submit Update** (on the Edit Freeze page) is clicked. The subject line of the email is the freeze name.

    When an email is sent, a freeze audit information log is checked into the repository. This log contains information about the freeze (freeze name, description, and creation date) and information about the e-mail notification sent (sender, recipient, message, and send date).

    Email cannot be sent if default metadata for checked-in audit logs has not been defined.
13. Enter an email message. Maximum characters allowed: 3000.
14. (Optional) Specify if notification should be periodically re-sent.
15. Select a period to wait before re-sending, and the period value (for example, 1 month).
16. Click **Create**.

    A message appears stating the freeze was created successfully, with the freeze information.
17. Click **OK**.

14.2.2 Editing a Freeze

Use the following procedure to edit a freeze:

1. Choose **Records** then **Configure** from the top menu.
2. Choose **Retention** then **Freezes**.
3. On the Freeze Configuration page, choose **Edit** then **Edit Freeze** from a freeze's **Actions** menu.
4. On the Create or Edit Freeze page, make modifications as required, and click **Submit Update** when done.

A message appears indicating the freeze was updated successfully, with the freeze information.

5. Click **OK**.

14.2.3 Viewing Freeze Information

> **Note:**
>
> The Admin.RecordManager right is required to perform this task. This right is assigned by default to the Records Administrator role.

1. Choose **Records** then **Configure** from the top menu.
2. Choose **Retention** then **Freezes**.
3. On the Freeze Configuration page, click a freeze name to view.
4. When done, click **OK**.

This page also has menu options to perform the following actions:

- **Edit**: Used to edit the current freeze, unfreeze the freeze, or alter the notification.
- **Delete**: Used to delete the current freeze.

> **Note:**
>
> You cannot delete a freeze if that freeze is currently applied to any content items. If you try, an error message is displayed.

- **Information**: Used to perform the following searches:
  - **Screen Frozen Content**: Displays a list of content items frozen with the current freeze. The list does not include any frozen content that inherited its freeze status from the parent record folder.
  - **Screen All Frozen Content**: Display a list of all content items frozen with the current freeze. The list also includes all frozen items that inherited their freeze status from their parent folders.
  - **Screen Frozen Folders**: Display a list of folders frozen with the current freeze. The list does not include any frozen folders that inherited their freeze status from their parent folders.
  - **Screen All Frozen Folders**: Display a list of all folders frozen with the current freeze. The list includes all frozen folders that inherited their freeze status from their parent folders.

> **Note:**
>
> The **Screen...** options are available only if you have the Admin.Screening right.

14.2.4 Deleting a Freeze

> **Note:**
>
> The Admin.RecordManager right is required to perform this action. This right is assigned by default to the Records Administrator role. Delete permission (D) for the security group of the freeze is also required.

A freeze cannot be deleted if the freeze is currently applied to any items. To delete a freeze:

1. Choose **Records** then **Configure** from the top menu.
2. Choose **Retention** then **Freezes**.
3. On the Freeze Configuration page, choose **Delete** from a freeze **Actions** menu.

To delete multiple freezes, select the freeze check box and choose **Delete** from the table menu on the Freeze Configuration page.

14.2.5 Freezing Items, Folios or Folders

> **Note:**
>
> The Admin.RecordManager right is required to perform this task. This right is assigned by default to the Records Administrator role.

To freeze a folder, content item or folio.

1. Search for and find the item to freeze.
2. On the Search Results page, select the item to freeze by selecting the check box next to the item name.

   A dialog opens. If changing the freeze that is in use, select a freeze from the list.
3. Choose **Edit** then **Freeze Selected** from the table menu.

   Select a freeze reason from the Freeze page. Freezes added to the user's Favorites list appear. To see all freezes, click the **Show All Freezes** link. Enter a reason for the freeze.
4. Click **OK**.

   A message appears indicating the items are frozen. To view frozen items after a freeze is executed from the Search Results page, click **Refresh** or execute a new search.
5. Click **OK**.

14.2.6 Unfreezing Frozen Items or Folders

> **Note:**
>
> The Admin.RecordManager right is required to perform this task. This right is assigned by default to the Records Administrator role.

To unfreeze all folders or content items currently frozen with a particular freeze:

1. Choose **Records** then **Configure** from the top menu.
2. Choose **Retention** then **Freezes**.
3. On the Freeze Configuration page, choose **Edit** then **Unfreeze** from a freeze's **Actions** menu.

   A dialog opens. If changing the freeze that is in use, select a freeze from the list. Freezes added to the user's Favorites list appear. To see all freezes, click the **Show All Freezes** link.
4. In the **Unfreeze Reason** field, specify a reason for the unfreeze action.
5. Click **OK**.

   A message appears stating all items with the selected freeze have been successfully unfrozen.
6. Click **OK**.

14.2.7 Searching for Frozen Content and Folders

> **Note:**
>
> The Admin.RecordManager right and Admin.Screening right is required to perform this task. These rights are assigned by default to the Records Administrator role.

To search for content items or folders currently frozen with a specific freeze:

1. Choose **Records** then **Configure** from the top menu.
2. Choose **Retention** then **Freezes**.
3. On the Freeze Configuration page, click the **Actions** menu for a freeze. In the **Information** page menu, choose one of the **Screen...** options:
   - **Screen Frozen Content**: Used to display a list of all content items currently frozen with the selected freeze. The list will not include any frozen content that inherited freeze status from a parent record folder. Either this option or the next option produce essentially the same result.
   - **Screen Derived Content**: Used to display a list of all content items currently frozen with the selected freeze and any items frozen in a folder with this

freeze. Therefore, the list includes all frozen items that inherited their freeze status from their parent folders.

- **Screen Frozen Folders**: Used to display a list of all folders currently frozen with the selected freeze. The list will not include any frozen folders that inherited their freeze status from their parent folders.
- **Screen All Frozen Folders**: Used to display a list of all folders currently frozen with the selected freeze. The list will also include all frozen folders that inherited their freeze status from their parent folders.

The Frozen Item page opens, listing all content or folders meeting the criteria of the selected screening option.

14.2.8 Re-Sending an Email Notification for a Freeze

> **Note:**
>
> The Admin.RecordManager right is required to perform this task. This right is assigned by default to the Records Administrator role.

If email notifications are set for a freeze, the notification email is first sent out when the freeze is created. Notifications can be sent periodically when a freeze is created.

To re-send the email notification about the freeze (for example, to notify the people involved about a change in the freeze implementation).

1. Choose **Records** then **Configure** from the top menu.
2. Choose **Retention** then **Freezes**.
3. On the Freeze Configuration page, click a freeze name.
4. On the Freeze Information page, make modifications to the email properties (recipients, message text) as required.
5. Click **Submit Update** when done.

   A message appears stating the freeze was updated successfully, with the freeze information. The notification email has been sent using default email settings.
6. Click **OK** to return to the Configure Retention Settings page.

Notifications can also be set by searching for a freeze. On the Freeze Information page, click **Edit** then **Renotify**.

14.2.9 Example: Creating a Freeze

This example creates a freeze due to litigation with a company. The freeze is valid until 2/20/2016.

1. Choose **Records** then **Configure** from the top menu.
2. Choose **Retention** then **Freezes**.
3. On the Freeze Configuration page, in the Freeze area, click **Add**.
4. On the Create or Edit Freeze page, in the Security Group field, verify that **RecordsGroup** is selected.

5. In the **Filer** field, verify that your own user login is displayed.
6. In the **Freeze Name** field, type **`Litigation`**.
7. In the **Freeze Description** field, type **`Litigation With Company XYZ`**.
8. In the **End Date** field, specify **`2/20/2016`** as the end date, by typing or using the calendar icon.
9. In the **Unfreeze Instructions** field, type **`Do not unfreeze until the litigation proceedings are completed`**.
10. If required, select **Send Notification** and provide the email properties (recipients, from-address, and message text).
11. Click **Create** when done.

14.3 Creating Dispositions

Disposition actions can include activities such as transfer to storage facilities or Federal records centers, transfer of permanent content to the National Archives and Records Administration (NARA), the disposal of temporary content, the replacement of content with updated information, and the adjustment of classifications.

Disposition is the last stage of three stages (creation/receipt, use and maintenance, disposition) in content life cycle. Dispositions are defined using disposition instructions. A disposition instruction is typically constructed as follows:

1. When a specified triggering event occurs (see Triggering Events).
2. Wait a specified period (the retention period, described in Retention Periods), if required, and then
3. Perform a specified disposition action (see Disposition Actions).

A disposition instruction is created within a retention category. All children record folders and content items normally inherit dispositions from their parent retention category, but a disposition rule can be applied to a specific record folder only.

Access Control Lists (ACLs) can affect what items a user can access when processing dispositions. For example, if a user is not in the ACL for a category, the user will not be able to access a pending disposition even if that user is in the appropriate alias group and has the appropriate rights and permissions. Always verify the ACL in use with a category to ascertain what effect it may have on actions taken on that category

This section discusses the following topics:

- Disposition Types
- Category Rule Review Using Workflows
- Triggering Events
- Retention Periods
- Disposition Actions
- Cutoff Guidelines
- Disposition Precedence
- Managing Dispositions
- Disposition Examples

14.3.1 Disposition Types

The following types of dispositions are available:

- Event Dispositions
- Time Dispositions
- Time-Event Dispositions

14.3.1.1 Event Dispositions

An *event disposition* is when items are eligible for disposition when an event takes place. Upon the occurrence of a specified event, or immediately thereafter, an item is eligible for the disposition. The event itself acts as a cutoff or closing occurrence. An event disposition does *not* have a retention period and uses actions like Delete Revision and Delete All Revisions. Typical examples of an event disposition instruction are Destroy When Obsolete or, in the case of classified content, Retain For Ten Years After Declassification. The disposition actions can vary.

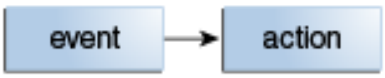
- Content that is tracked for DoD purposes use actions like Destroy and Retain, and the states of the items are Obsolete and Declassified, respectively.
- Non-DoD content uses actions like Delete Revision and Delete All Revisions.

To view an example step-by-step procedure for creating an event disposition, see Event Disposition.

If classification is used (an optional security feature that is also certified to comply with the Chapter 4 requirements of the DoD 5015.2 specification), an event disposition can be set to declassify content on a specific date or downgrade classification on a specific date.

To summarize, event dispositions do not have retention periods and have an implicit, system-derived cutoff.

Figure 14-1 Event Disposition



14.3.1.2 Time Dispositions

A *time disposition* has a fixed retention period and begins with a user-defined file cutoff. The retention period must transpire before the disposition instruction takes action on the content item. Typical examples include the following:

- Cutoff at the end of the (fiscal or calendar) year
- Retain for three years, then destroy
- Cut off at declassification, retain for ten years, then destroy (DoD classified items)

To view an example step-by-step procedure for creating a time disposition, see Time Disposition.

To summarize, time dispositions have retention periods and explicitly defined cutoffs.

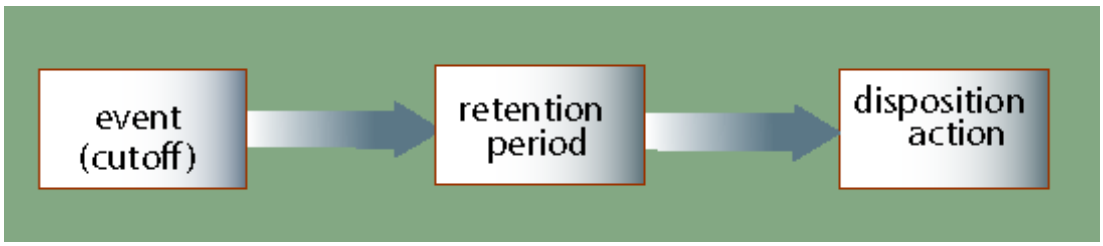
Figure 14-2 Time Disposition

14.3.1.3 Time-Event Dispositions

A *time-event disposition* is a disposition instruction beginning with a specified triggering event. After the event has transpired, then the folder or content item is cut off and the retention period is applied. A typical example of a time-event disposition instruction is *Destroy five years after a (legal) case is closed*. To view an example step-by-step procedure for creating a time-event disposition, see Time-Event Disposition.

To summarize, time-event dispositions have explicitly defined events, cutoffs, and retention periods.

Figure 14-3 Time-Event Disposition



14.3.2 Category Rule Review Using Workflows

The category rule review functionality must be enabled before the disposition is available for general use. To use this feature, the following configuration variables must be set:

- Select **Enable Category Dispositions Reviews** on the Configure Retention Settings page.
- **CategoryDispositionWorkflowContentType**: The default workflow for category dispositions is performed by the retention category content type. Alter this configuration variable to a different content type if needed.
- **UpdateDispositionTableOnWorkflowApproval**: Allows the system to update the dispositions table when the workflow is processed and approved. The default is true. If set to false, the table is updated when the content item is released. If a final revision is deleted, the previous revision becomes the current revision and when that revision is released, the dispositions table is updated.

Workflows must be set up to enable the review of disposition rules. Enable the workflow to initiate workflow processing. Once enabled, items proceed into a workflow. If the process is disabled before the items finish the workflow process, the items may stay in the workflow and not complete until the process is enabled again.

After the functionality is enabled, dispositions enter a workflow for approval before use. After creating a disposition, a message is displayed indicating the disposition is in the workflow, awaiting approval.

14.3.3 Triggering Events

A disposition instruction is activated when a triggering event occurs. The following types of triggering events can occur:

- Preceding Actions Triggering Event: an event in which an action such as the following precipitates the event:
  - **Retention Period Cutoff**: This event cuts off disposition processing and applies a retention period. It can be used for system-derived triggering events based on time dispositions or time-event dispositions.
  - **Period Cutoff with Volume**: This event cuts off disposition processing to a volume and applies a retention period.
- Content State Triggering Event: an event in which content status such as the following sets the trigger:
  - **Canceled**: This event is activated when the associated content or record folders have been canceled.
  - **Delete Approved**: This event is activated when the associated content or record folders have been approved for deletion.
  - **Expired**: This event is activated when the associated content or record folders have been expired.
  - **Obsolete**: This event is activated when the associated content or record folders have been marked as obsolete.
  - **Obsolete and Delete Approved**: This event is activated when the associated content or record folders have been marked as obsolete and have been approved for deletion.
  - **Rescinded**: This event is activated when the associated content or record folders have been rescinded (that is, made void because of an enacting authority).
  - **Superseded**: This event is activated when the associated content has been superseded that is, supplanted, or displaced, by content that is more recent or improved).

    > **Note:**
    >
    > Items must be linked to be superseded.

  - **No Longer Latest Revision**: This event is activated when the associated content revisions are no longer the latest revision (that is, a new revision has been checked into the repository). This trigger enables a user to create a rule to initiate automatic disposal of old revisions of content. This is especially useful to keep only the latest revision of content, and automate the disposal of old revisions.
  - **Superseded Twice**: This event is activated when the associated superseded content are superseded again. If content item A is superseded by content item B, which is subsequently superseded by content item C, then this trigger is activated for content item A.
  - **Last New Record Added**: This event is activated when the associated item is the most recent item added to a record folder. This enables a user to track the activity in

a folder, which can be useful to optimize the usage of folders based on their activity level. For example, you may decide to delete (or otherwise process) folders if there has been no activity for a specified period.

  - **Scheduled declassify date**: This event is activated when the associated content or record folders are scheduled to be declassified on a specific date. This trigger is available only if the ClassifiedEnhancements component is enabled.
  - **Scheduled downgrade date**: This event is activated when the associated content or record folders are scheduled to be downgraded in their security classification on a specific date. This trigger is available only if the ClassifiedEnhancements component is enabled.
  - **Declassified date**: This event is activated when the associated content or record folders have been declassified on a specific date. This trigger is available only if the ClassifiedEnhancements component is enabled.
- Indirect Triggers: An event is activated when the associated content or record folders have been approved during an audit (using the built-in Audit Approval indirect trigger).
- Custom Triggers: See Types of Triggers for details about custom triggers.

14.3.4 Retention Periods

The retention period is the amount of time waited after the triggering event before a disposition action is performed. Several built-in period units (including calendar years, fiscal quarters, months, and weeks) are available, but custom periods can be created.

A retention period can be specified for all triggering events, enabling a user to create disposition rules for content such as *Delete all old revisions three months after the last new revision was checked in*.

Examples of retention periods include:

- 5 calendar years
- 2 fiscal quarters
- 6 months
- 4 weeks

14.3.5 Disposition Actions

A disposition action defines what will happen after Triggering Events occur and Retention Periods, if any, have passed. The following built-in disposition actions are supported. In addition to the built-in disposition actions below, a user can define custom disposition actions.

The following actions are discussed:

- Classified Records Actions
- Dispose Actions
- Other Actions
- Transfer/Move Actions

> **Note:**
>
> Default disposition actions always require approval from an administrator. Custom disposition actions can be configured to perform approvals automatically. Some actions have a separate Mark Complete step because the system cannot tell if the action is done.
>
> For example, the completion of destruction or moves of physical records cannot be determined by the software, so someone must mark the action complete. The same is true for all transfer, accession, and move actions where the destination is defined using the software and the physical movement of the items is not within control of the software.

14.3.5.1 Classified Records Actions

- **Declassify**: This action indicates it is time to declassify content.
- **Downgrade Classification**: This action indicates it is time to lower the security classification of an item to the next lower security classification in the hierarchy.
- **Review Classification**: This action indicates it is time to review the security classification status of an item.
- **Upgrade Classification**: This action indicates it is time to increase the security classification of an item to the next higher security classification in the hierarchy.

These four disposition actions are available only if the ClassifiedEnhancements component is enabled.

14.3.5.2 Dispose Actions

- **Delete Previous Revision**: This action indicates it is time to delete the revision before the content item revision that triggered the disposition action. The revision that activated the trigger may be the latest revision of a content item, but does not need to be.
  - If a content item has 5 revisions and this disposition action is activated for revision 5 (the latest revision), then only revision 4 is marked for deletion.
  - If a content item has 5 revisions and this disposition action is activated for revision 3, then only revision 2 is marked for deletion.
- **Delete Revision**: This action indicates it is time to delete the content item revision that triggered the disposition action. This revision may be the latest revision of a content item, but does not need to be.
  - If a content item has 5 revisions and this disposition action is activated for revision 5 (the latest revision), then only revision 5 is marked for deletion.
  - If a content item has 5 revisions and this disposition action is activated for revision 3, then only revision 3 is marked for deletion.
- **Approve Deletion**: This action indicates it is time to approve record folders or content for deletion.
- **Delete All Revisions**: This action indicates it is time to delete the content item and all its associated revisions. The revision that activated the trigger may be the latest revision of a content item, but does not need to be. If the DoD Config module is enabled, a prompt appears to select either **Delete All Revisions (Destroy Metadata)** or **Delete Revisions**

(Keep Metadata) when approving the disposition action. Metadata cannot be retained unless the DoD Config module is enabled.

  - If a content item has 5 revisions and this disposition action is activated for revision 5 (the latest revision), then revisions 1 through 5 are marked for deletion (effectively removing the content item from the repository altogether).
  - If a content item has 5 revisions and this disposition action is activated for revision 3, even then, all revisions 1 through 5 are marked for deletion.

- **Delete Old Revisions**: This action indicates it is time to delete all revisions before the content item revision that triggered the disposition action. The revision that activated the trigger may be the latest revision of a content item, but does not need to be.
- **Delete Working Copy**: This action deletes the working copy of a cloned content item. It first deletes the direct working copy of the clone. Then all previous revisions of the working copy are deleted until a revision of the fixed clone itself is found. The deletions stop at that point. This action is not available unless the `RmaEnableFixedClones` configuration variable is set to true.

If deletion rules exist for a category, content is deleted according to the first rule encountered. Therefore, content is deleted from all folders in the same category and not just from one folder.

14.3.5.3 Other Actions

- **Check in New Revision**: This action indicates it is time to take the latest revision of the affected content items and check a copy of this revision into the repository as a new revision. This may be useful to process a content item revision based on changed historical information, refresh an expired document, or enter a content item into a criteria workflow for disposition processing.
- **Accession**: This action indicates it is time to transfer physical and legal custody of materials to an archival institution such as NARA. Choose **Accession (Destroy Metadata)** or **Accession (Keep Metadata)**.
- **Activate**: This action indicates it is time to activate record folders or content.
- **Close**: This action indicates it is time to close record folders.
- **Cutoff**: This action indicates it is time to cut off content or record folders from further processing. Cutoff refers to changing the status of items to prohibit further processing.
- **Cutoff and Create Volume**: This creates a volume folder, content is placed inside, and the volume is cut off.
- **Expire**: This action indicates it is time to expire record folders or content.
- **Obsolete**: This action indicates it is time to mark content as obsolete.
- **Mark Related Content**: This action marks any content linked to the current content.
- **No Action**: This action indicates there is no action to take currently. This action usually found mid-disposition. A No Action action acknowledges a disposition milestone has passed, and the next step in the disposition begins processing.
- **Notify Authors**: This action indicates it is time to notify the author of the affected category that disposition actions are due for the category.

- **Supersede**: This action indicates it is time to supersede a content item by another content item.

In addition to the built-in disposition actions listed above, custom dispositions can be defined to reflect an organization's specific records management needs.

14.3.5.4 Transfer/Move Actions

- **Archive**: This action indicates it is time to archive content or record folders. Choose **Archive (Destroy Metadata)** or **Archive (Keep Metadata)**.
- **Create Content Server Archive**: This action indicates it is time to create an archive containing the affected content with their metadata.
- **Create Volume**: Creates a volume folder. When the action is encountered, the contents are transferred to the volume folder.
- **Move**: This action indicates it is time to move content and metadata out of the system. Choose to **Move (Destroy Metadata)** or **Move (Keep Metadata)**.
- **Transfer**: This action indicates it is time to transfer content from one location to another, but does not transfer the legal and physical custody (as with accession). Choose to **Transfer (Destroy Metadata)** or **Transfer (Keep Metadata)**.

14.3.6 Cutoff Guidelines

In most cases, a retention period does not start until a triggering event is set to **cut off**. To cut off the records in a file indicates record revisions are ended at regular intervals to permit disposal or transfer in complete blocks. For correspondence files, this permits the establishment of new files. Cutoffs involve ending input to old files and starting input to news ones.

The length of the retention period determines when to cut off a content item, category, or folder and at what interval to perform a cutoff. Use the guidelines discussed in this section to help determine when to cut off and apply retention periods.

Retention periods for triggers can only be specified if the `AllowRetentionPeriodWithCutoff` variable is enabled. It is disabled by default.

14.3.6.1 Time Retention Periods

Content items that have a retention period of less than one year are typically cut off at an interval equal to the retention period. For example, if a retention category has a retention period of one month, cut the folder off at the end of each month. Then, apply the retention period for another month before applying the final disposition, such as destroying the items.

When a content item has a retention period of one or more years, cut off the folder at the end of each fiscal or calendar year. After the end of year cutoff, apply the retention period.

14.3.6.2 Time-Event Retention Periods

On the date the event or action is completed, perform the cutoff, then apply the retention period.

14.3.7 Disposition Precedence

Content filed into multiple folders residing in different categories are managed based on the longest time disposition.

When an item has been filed into multiple folders belonging to disparate retention categories, it is subject to multiple disposition processing schedules. In the event of this scenario, the longest retention period prevails. However, the item is processed by disposition instructions belonging in two or more categories. The following scenario describes a disposition processing precedence.

Content is filed into Folder 1 of Category 1 and into Folder 2 of Category 2.

Category 1: Folder 1	**Category 2: Folder 2**
Expire after 4/1/12	Close after 3/1/12
Archive on 4/10/12	Expire after 4/5/12
Destroy on 4/12/12	Destroy on 4/20/14

The instructions are processed in a staggered order:

1. On 3/1/12, the item will be cutoff with its cutoff date and Folder 2 will be closed.
2. On 4/1/12, the item will be expired and the expiration date will be added to the item (viewable on the content information page).
3. On 4/5/12, the item will not be expired again, so the expiration date is not updated.
4. On 4/10/12, the item and Folder 1 will be archived.
5. On 4/12/12, the pointer to the item is removed from Folder 1 by an update to the content information. The pointer still exists to Folder 2. The items are not actually filed into a folder, but are pointed to the folder.
6. On 4/20/14, the item under Folder 2 will finally be destroyed, as the item is not being held by any remaining pointers.

14.3.8 Managing Dispositions

The following tasks are involved in managing dispositions:

- Enabling or Disabling User-Friendly Captions
- Creating a Disposition Rule
- Editing a Disposition Rule
- Copying a Disposition Rule
- Viewing Disposition Information
- Deleting a Disposition Rule

14.3.8.1 Enabling or Disabling User-Friendly Captions

> **Note:**
>
> The Admin.RecordManager right is required to perform this action. This right is assigned by default to the Records Administrator role.

User-friendly captions can be enabled or disabled at any time. This setting also affects the query strings in the Criteria boxes of the Screening pages.

To enable or disable user-friendly captions:

1. Choose **Records** then **Configure** from the top menu.
2. Choose **Retention** then **Settings**.
3. On the Configure Retention Settings page, expand the User Interface section if necessary. Select **User-Friendly Disposition**.
4. Click **Submit Update**.

   A message appears stating the configuration was successful.
5. Click **OK**.

14.3.8.2 Creating a Disposition Rule

> **Note:**
>
> The Category.Create right is required to perform this action. This right is assigned by default to the Records Administrator role.

A disposition rule applies to all content and record folders in a category by default. A disposition rule can also be created that applies only to a specific record folder. This is a general navigational procedure; to view example procedures for specific types of dispositions, see Disposition Examples.

1. Click **Browse Content** then **Retention Schedules**.
2. In the row for the retention category on the Exploring Retention Schedule page, choose **Edit** then **Edit Disposition** from the item's **Actions** menu.

   The (initially blank if creating a disposition) Disposition Instructions page opens.
3. In the Disposition Instructions area, click **Add**.
4. On the Disposition Rule page, choose the disposition rule's triggering event from the Triggering Event (After) list.
5. If the disposition rule has a retention period, enter an integer value for Retention Period (Wait for) and select the corresponding period from the Retention Period list.

   Required or optional depending on the disposition instruction scenario. For retention categories, a user can specify a retention period only for the Retention Period Cutoff and

Preceding Action triggering events. For content item categories, a user can specify a retention period for all triggering events. With this functionality, a user can create disposition rules for content such as *Delete all old revisions three months after the last new revision was checked in*.

6. Select an action for the rule from the Disposition Action (Do) list. The system sends an email message to the person responsible for performing this action.
7. (Optional) If a user other than the category author should review the email notifications triggered by the disposition rule, specify the user in the **Notification Reviewer** field by entering the user name or selecting a user from the list next to the field. If not specified, only the category author is notified of events triggered by the disposition rule. If specified, it depends on the software configuration who will receive email notifications, either the specified user and the category author (the default) or the specified user only.
8. If the item should go through an external approval process, select the check box. This option only appears if an external approval process has been set up on the system (for example, if a record on an external system is to be managed by the local system without being physically present).
9. (Optional) Click the plus symbol (+) to expand the lower section of the screen. If the disposition instruction applies only to a specific record folder, select the folder from the Apply to Folder (On Folder(s)) list. Otherwise, allow the instruction to apply to all folders within a category.
10. (Optional) If the disposition instruction applies only to other retention objects, select an object from the list. Otherwise it will apply to all objects.
11. (Optional) When creating a category disposition using Accession, Archive, Move, or Transfer, a field is available to designate how archiving is to be done through the Location Type list.

    When an item is archived to an external storage location using File Storage, FTP, or WebDAV, the metadata audit history is included with the item's metadata. Select an alternate metadata path if needed. If the alternate metadata path required authentication, it must match that of the primary archive path. A user can elect to be prompted for this information or use default information provided in the user profile, as discussed below.

    WebDAV will support a PropPatch method that assigns meta values to a file that has been uploaded to a WebDAV server. To enable this functionality, a configuration variable must be set.

    By default when the action is performed, a zip file containing the items associated with the disposition is placed in the storage location. Select the box to unpack the zip file at destination.

    Depending on the location type chosen, fill in the following information:

    - **File Storage**: Enter the storage path for the archive file.
    - **FTP**: Specify the path to the FTP server and the directory location for the archive and, if chosen, the meta path. Enter the appropriate user name and password.
    - **WebDAV**: Specify a valid WebDAV path and, if chosen, the meta path. Enter the appropriate WebDAV user name and password.
    - **Other**: This selection specifies that the archive will download manually when the action is performed. If the destination has an associated location or container, enter a description in the appropriate text box.

Items can also be transferred to an external workspace. Set up the external workspace by clicking **My Profile**. Click **Edit** next to the User Workspace caption. An external workspace can be a local file system, a FTP server, a WebDAV server, or a manual download and can be set up in the same way the Location Type is set up here.

> **Note:**
>
> You can set defaults for the location type for each user. Click the user name in the top right corner of the screen. The My Profile page opens. Click **Edit** in the User Workspace section. You can set default locations, passwords, and other details for the location types there.

12. If necessary, choose a physical container for an external record folder, such as a barcode or some other means of identification. Maximum characters: 30.
13. If necessary, map fields when exporting data to another system that may have metadata fields with different names. Field mapping can be used when creating the meta file for export. If a field is mapped, then the mapped name are used in the file instead.
14. After making selections if necessary reorder the instructions in the list. If Cutoff is present, it must be the first rule. If the Destroy or Accession rule is present, those rules must be last.To reorder an instruction, select it in the list, and click the up or down arrow.
15. Click **Submit Update**.

    A message appears with the disposition information.
16. Click **OK**.

> **Note:**
>
> The Category.Edit right is required to perform this action. This right is assigned by default to the Records Administrator role.

14.3.8.3 Editing a Disposition Rule

To edit a disposition rule within the disposition instructions for a retention category:

1. Choose **Browse Content** then **Retention Schedules**.
2. On the Exploring Retention Schedule page, navigate to the appropriate retention category.
3. Choose **Edit** then **Edit Disposition** from the item's **Actions** menu.
4. On the Disposition Instructions page, select the rule to edit, and click the **Edit** icon (an image of a pencil).
5. Make changes to the rule on the Disposition Rule page and click **OK**. The Disposition Rule page closes.
6. Click **Submit Update**.

   A message appears with the disposition information.
7. Click **OK**.

14.3.8.4 Copying a Disposition Rule

> **Note:**
>
> The Category.Create right is required to perform this action. This right is assigned by default to the Records Administrator role.

To copy rules from other categories to overwrite the ones in a current category:

1. Choose **Browse Content** then **Retention Schedules**.
2. Navigate to the appropriate retention category on the Exploring Retention Schedule page.
3. In the row for the retention category, choose **Edit** then **Copy Disposition From** from the item's **Actions** menu.

   A prompt appears, asking permission to overwrite the rules with rules from another category. Click **OK** to continue.
4. The Browse for Category page opens. This is similar to the Select Retention Series, Record Folder or Category dialog. Choose a category in the list from which to copy a disposition rule.
5. If needed, edit the rules on the Disposition Instructions page in the same manner as described earlier.
6. Click **Submit Update**.

   A message appears with the disposition information.
7. Click **OK**.

14.3.8.5 Viewing Disposition Information

> **Note:**
>
> The Category.Read right is required to perform this action. This right is assigned by default to the Records Administrator role.

1. Choose **Browse Content** then **Retention Schedules**.
2. Navigate to the appropriate retention category on the Exploring Retention Schedule page.
3. In the row for the retention category, click the **Info** icon.
4. When done, click **OK**.

14.3.8.6 Deleting a Disposition Rule

> **Note:**
>
> The Category.Delete right is required to perform this action. This right is assigned by default to the Records Administrator role.

To delete a disposition rule from within a category, or to delete the entire set of disposition instructions:

1. Choose **Browse Content** then **Retention Schedules**.
2. Navigate to the appropriate retention category on the Exploring Retention Schedule page.
3. In the row for the retention category, click **Edit** then **Edit Disposition**.
4. On the Disposition Instructions page, select the rule to delete and click the Delete icon (a red x in a circle).
5. The rule is deleted from the list. Repeat for each rule to delete.
6. Click **Submit Update**.

   A confirmation message appears.
7. Click **OK**.
8. It is advisable to run the Batch Services after deleting a disposition rule in order to recompute disposition actions. Batch services are run automatically or can be initiated by selecting the appropriate action by choosing **Records** then **Batch Services** from the top menu.

14.3.9 Disposition Examples

This section includes the following disposition examples:

- Event Disposition
- Simple Time/Event Disposition
- Time Disposition
- Time-Event Disposition
- Disposition Rules for Specific Folders
- Multi-Phased Disposition

All of the examples in this section use the default (that is, non user-friendly) disposition captions.

14.3.9.1 Event Disposition

This example creates an event disposition instruction that destroys content after an event. The event is the content becomes obsolete. The disposition action is to destroy the content. This example requires creating one disposition rule.

Disposition instruction: Destroy when obsolete.

1. Navigate to the appropriate retention category.
2. In the row for the retention category, choose **Edit** then **Edit Disposition** from the item's **Actions** menu or click the **Info** icon and choose **Edit** then **Edit Disposition** from the page menu on the Retention Category Information page.

   The (initially blank) Disposition Information page opens.
3. In the Disposition Instructions area, click **Add**.
4. On the Disposition Rule page, in the Triggering Event list, click the **Obsolete** option.
5. In the Disposition Action list, click the **Destroy** option.
6. Click **OK**.

   The disposition rule is displayed in the Disposition Instructions box.
7. Click **Submit Update**.

   A confirmation message appears.

14.3.9.2 Simple Time/Event Disposition

This example demonstrates creating a disposition based on an item's revision status.

Disposition Instructions: When a new version of an item is checked in, wait one week and notify the original author.

1. Navigate to the appropriate category.
2. In the row for the retention category, choose **Edit** then **Edit Disposition** from the item's **Actions** menu or click the **Info** icon and choose **Edit** then **Edit Disposition** from the page menu on the Retention Category Information page.
3. On the Disposition Instructions page, in the Disposition Instructions area, click **Add**.
4. On the Disposition Rule page, in the Triggering Event list, select **No Longer Latest Revision**. The Retention Period field becomes available.
5. In the Retention Period fields, enter 1 and select **Weeks** from the Retention Period list.
6. In the Disposition Action list, click the **Notify Authors** option.
7. Click **OK**.

   The disposition rule is displayed in the **Disposition Instructions** box.
8. Click **Submit Update**.

   A completion message appears.

14.3.9.3 Time Disposition

This example demonstrates creating a time disposition with a retention period and a final disposition of destroying content. There is a predictable event trigger commencing at the end of a fiscal year.

Disposition Instructions: Cut off at the end of the fiscal year, hold for three fiscal years in the current file area, then destroy.

1. Navigate to the appropriate category.
2. In the row for the retention category, choose **Edit** then **Edit Disposition** from the item's **Actions** menu or click the **Info** icon and choose **Edit** then **Edit Disposition** from the page menu on the Retention Category Information page.
3. In the Disposition Instructions area of the Disposition Instructions page, click **Add**.
4. In the Triggering Event list on the Disposition Rule page, click the **Retention Period Cutoff** option. The Retention Period field becomes available.
5. In the Retention Period field, enter 3 and select **Fiscal Years** on the Retention Period list.
6. In the Disposition Action list, select the **Destroy** option.
7. Click **OK**.

   The disposition rule is displayed in the **Disposition Instructions** box.
8. Click **Submit Update**.

   A confirmation message appears.

Notice this disposition uses a system-derived triggering event. After the item becomes obsolete, it is automatically cut off at the end of the fiscal year then the retention period begins.

14.3.9.4 Time-Event Disposition

A typical example of a time-event disposition instruction is *Destroy five calendar years after the (legal) case is closed*. A time-event disposition is different from a time disposition because the exact time the event might occur cannot be predicted, but when it does, the disposition processing begins. A time-event disposition also uses a built-in or custom trigger. When the event occurs, the activation date for the custom trigger is entered, if applicable.

This example creates an event disposition instruction that destroys items at a specified time after an event. The event is the closing of a pending legal case. The retention time period is five years. The disposition action is to destroy the content.

This example requires creating a custom trigger called Case Closed. Create a custom trigger without an activation date. After the case is closed, you would also need to go in and set the activation date for the custom trigger.

Disposition Instructions: Destroy five calendar years after case closed.

1. Navigate to the appropriate category.
2. In the row for the retention category, choose **Edit** then **Edit Disposition** from the item's **Actions** menu. You can also click the Info icon and choose **Edit** then **Edit Disposition** from the page menu on the Retention Category Information page.
3. In the Disposition Instructions area on the Disposition Instructions page, click **Add**.
4. Define the first disposition rule on the Disposition Rule page.
   a. In the Triggering Event list, select the **Case closed** option under the Custom Triggers sublist.
   b. In the Disposition Action list, select the **Cutoff** option.
   c. Click **OK**.

      The rule is displayed in the Disposition Instructions box.
5. Define the second disposition rule.

a. Click **Add** to add another rule.

b. In the Triggering Event list, select the **Preceding Action** option under the **Preceding Action** sublist.

c. In the Retention Period field, specify 5 calendar years.

d. In the Disposition Action list, select the **Destroy** option.

e. Click **OK**.

The rules are displayed in the Disposition Instructions box. Notice the rule prefaced by a preceding action is indented with an ellipsis.

6. Click **Submit Update**.

A completion message appears.

14.3.9.5 Disposition Rules for Specific Folders

This example demonstrates creating a disposition instruction that applies different rules to the folders within a category.

Disposition Instructions: Close the folder to further filing after a specified event, and then destroy.

- Folder 1: Event trigger is Program ABC canceled.
- Folder 2: Event trigger is Program BBC expired.
- Folder 3: Event trigger is Program CDB rescinded.

This example requires creating three record folders (F1, F2, F3) and a custom event trigger for each folder. Each folder contains correspondence relevant to a particular program.

1. Navigate to the appropriate category.
2. In the row for the retention category, choose **Edit** then **Edit Disposition** from the item's **Actions** menu. You can also click the **Info** icon and choose **Edit** then **Edit Disposition** from the page menu on the Retention Category Information page.
3. In the Disposition Instructions area on the Disposition Instructions page, click **Add**.
4. Define the first disposition rule for record folder 1 on the Disposition Rule page.

a. In the Triggering Event list, select **Program ABC Canceled**, the custom trigger you created for the folder.

b. In the Disposition Action list, select the **Destroy** action.

c. In the Advanced Options section, select **Folder 1**, the folder which will have the rule applied.

d. Click **OK**. The rule is displayed in the Disposition Instructions box.

5. Define the second rule for record folder 2.

a. Click **Add** to add another rule.

b. In the Triggering Event list, select **Program BBC Expired**, the custom trigger you created for the folder.

c. In the Disposition Action list, select the **Destroy** action.

d. In the Advanced Options section, select **Folder 2**, the folder which will have the rule applied.

e. Click **OK**. The rule is displayed in the Disposition Instructions box.

6. Define the second rule for record folder 3.
   a. Click **Add** to add another rule.
   b. In the Triggering Event list, select **Program CDB Rescinded**, the custom trigger you created for the folder.
   c. In the Disposition Action list, select the **Destroy** action.
   d. In the Advanced Options section, select **Folder 3**, the folder which will have the rule applied.
   e. Click **OK**.

      The rule is displayed in the Disposition Instructions box.
7. Click **Submit Update**.

   A completion message appears. Notice there are rules drawn between the multiple instructions.

14.3.9.6 Multi-Phased Disposition

This example demonstrates defining a disposition instruction that has more phases than is typical in a disposition instruction. This example contains the disposition actions of move, transfer, and accession. A Move disposition action does not transfer the legal responsibility of content, whereas a Transfer disposition action does transfer both legal responsibility and physical location of content.

Disposition Instructions: Cut off at the end of the calendar year and hold for on year in the current file area, move to off-line storage for on year, transfer to the FRC (Federal Records Center) and retain for ten years, then final accession to NARA.

1. Navigate to the appropriate category.
2. In the row for the retention category, click **Edit** then **Edit Disposition** from the item's **Actions** menu. You can also click the Info icon and click **Edit** then **Edit Disposition** from the page menu on the Retention Category Information page.
3. In the Disposition Instructions area on the Disposition Instructions page, click **Add**.
4. On the Disposition Rule page, define the first phase of the disposition, which is cut off at the end of the calendar year, retain in the current file area for one year, and then move to offline storage.
   a. In the Triggering Event list, select the **Retention Period Cutoff** option. The Retention Period field becomes available.
   b. In the Retention Period fields, enter 1 in the text box and select **Calendar Years** from the Retention Period list.
   c. In the Disposition Action list, select the **Move** option to move the content to offline storage.
   d. In the Destination Location box, select **Offline Storage**.
   e. Click **OK**.

      The rule is displayed in the Disposition Instructions box.
5. Define the next phase of the disposition, which is transfer to the Federal Records Center after a one year retention period of offline storage.

a. Click **Add** to add another rule.

b. In the Triggering Event list, select the **Preceding Action** option.

c. In the Retention Period fields, enter 1 and select **Calendar Years** from the Retention Period list.

d. In the Disposition Action list, select the **Transfer** option to move the content to offline storage.

e. In the **Destination Location** box, type FRC.

f. Click **OK**.

The rule is displayed in the Disposition Instructions box, indented under the previous rule.

6. Define the final phase of the disposition, which is accession to the National Archives (NARA) after a ten year retention of the content in the FRC.

a. Click **Add** to add another rule.

b. In the Triggering Event list, select the **Preceding Action** option.

c. In the Retention Period field, enter 10 in the text box and select **Calendar Years** from the Retention Period list.

d. In the Disposition Action list, select the **Accession** option.

e. In the Destination Location box, type NARA.

f. Click **OK**.

The rule is displayed in the Disposition Instructions box, indented under the previous rule.

7. Click **Submit Update**.

A completion message appears.

8. Click **OK**.

14.4 Processing Dispositions

This section describes how dispositions are processed and what approvals may be needed in order for some specific types of disposition actions to proceed.

A user can quickly access retention assignments by choosing **Records** then **Approvals** from the top menu. They can also be accessed by choosing **My Content Server** then **My Records Assignments** from the main menu.

This section discusses the following topics:

- Items Subject to Review
- Approval and Completion
- Frozen Items and Event Processing
- Searching Retention Steps and Actions
- Using Batch Processing
- Specifying an Alternate Reviewer
- Managing Disposition Tasks

- Pending Event Processing
- Processing Dispositions

14.4.1 Items Subject to Review

Content can be subjected to periodic review whether it is managed in a disposition or not. From a DoD perspective, contents subject to review are vital. According to NARA, the National Archives and Records Administration in the United States, vital records are essential government agency content needed to meet operational responsibilities under emergency or disaster conditions, or are required to protect legal and financial rights of the Government. and update for any purpose so designated.

Organizations that are not government agencies may have content that is vital to their type of business and therefore subject to review.

Items that are subject to review typically comprise about five percent of content deemed critical to a business. Some examples of content of this type include:

- Software source code
- Patents and copyrights
- Legal documents such as trusts, estates, and wills
- Regulatory compliance data

Cycling vital content that is subject to review refers to the periodic replacement of obsolete copies of content with copies of current content. Initial reviews are based on the content release date content and the filing date for record folders. The next review date is based on the reviewer's last review date.

To find items awaiting review choose **Records** then **Approvals** from the top menu. Choose **Pending Reviews**.

If you are a member of the RmaReviewers alias, choose **List All** on the table menu on the page. This shows all items awaiting review and the person assigned to do those reviews. Choose **List Mine** to show only those items awaiting the logged-in user's approval.

14.4.2 Approval and Completion

Some pending triggering events require only approval by the person specified as the Notification Reviewer when the disposition was first set for the category. After the action has been approved, it is marked as such and is processed when dispositions are run, usually overnight. The disposition actions are logged in the audit log and are subsequently removed from the approval list.

Some events require two steps, depending on the event type and the item to be processed. First, they must be approved and after an action has been carried out manually, they must be marked as completed after the required event action has been executed (for example, physical transfer to a different location).

To view items awaiting disposition choose **Records** then **Approvals** from the top menu. Choose **Pending Dispositions**. To also access pending dispositions choose **My Content Server** then **My Records Assignments** from the main menu.

14.4.3 Frozen Items and Event Processing

After an event has been processed (approved and marked as completed if required) it should automatically be removed from the pending event pages (approval list and/or completion list). If an event remains on these pages there is probably a frozen item or folder preventing its removal.

For example, if a total of ten items are affected by a Destroy event and one of them is frozen, then the event for that one item will remain in the approval list, and the event will move to the completion list for the other nine items. These nine items can then be destroyed and the event marked as completed, but the frozen item cannot be processed until it is unfrozen.

For information about how to find those dispositions that did not succeed, see Viewing Failed Dispositions.

14.4.4 Searching Retention Steps and Actions

Use the Retention Step Search page to screen for disposition steps. For example, a user can screen to discover what actions have been approved, who approved them, and what actions are done. From the screening results, a report can be created that can then be used as a destruction certificate, if needed. To access this page, choose **Records** then **Audit** then **Retention Steps** from the top menu.

Information can also be displayed about any disposition actions that did not process correctly. The Failed Dispositions page shows those dispositions actions that did occur as specified. To access this page, choose **Records** then **Audit** then **Fail Dispositions** from the top menu. For details, see Viewing Failed Dispositions.

14.4.5 Using Batch Processing

Pending events and review cycles are processed by the system every night on a 24-hour cycle. Notifications are sent daily at midnight.

Use the **Batch Services** options on the **Records** menu to process certain actions immediately rather than wait for the scheduled processing time. Options on the **Batch** menu include:

- **Run All**: Processes all events pertaining to reviews or dispositions
- **Process Dispositions**: Processes all disposition-related pending events
- **Process Reviews**: Processes pending reviews regardless of whether items are in a disposition or not.
- **Send Notifications**: Sends any pending notifications relating to dispositions
- **Run Other**: Processes other batch services unrelated to disposition processing such as notification of monitoring alerts, scheduled key rotation, and so on.

The system default Scheduled Batch Services are processed every night at midnight and continue until the processing is finished. The time when these services run is controlled by a resource include. The include is found in the `records_management_resources.htm` file and is called `set_doevent_for_records_daily_event`. The timing could be changed by writing a component that overrides this include and changes when the processing runs.

The Batch Jobs that run during this time are:

- Processing all dispositions that are due for approval. After processing they will become pending so that a user can approve them.
- Processing all dispositions that have been approved and executing the disposition. After processing the disposition action will have been carried out. For example, items that are to be deleted will have been removed from Records.
- Various notifications that are to be sent to users such as vital reviewers and so forth will be completed, and the users will be notified of actions that need to be taken.

14.4.6 Specifying an Alternate Reviewer

It may be useful to select another user than yourself to perform review actions and process disposition events, for example when you are out of the office for some time. Alternate reviewers can be specified in your user profile. They will then receive email notifications of any pending actions assigned to you and can act on them.

Log in and open your user profile. Select an alternate reviewer from the list. The list includes all users who have been specified as default notification recipients. The selected person will now receive email notifications of pending actions and events assigned to you.

> **Note:**
>
> You can also specify an alias or a script to send the notification details of dispositions to more than one user, or multiple alternate reviewers. To achieve this, specify the alias:<alias name> or script:<script name> in the reviewer field. For example, alias:RmaReviewers.

By default, only the alternate reviewer will receive notifications and not the users. The system can be configured so both the users and the alternate reviewer are notified. To accomplish this, add the following to the `config.cfg` configuration file:

```
RmaNotifyReviewerAndAlternateReviewer=true
```

Restart Content Server for this setting to take effect.

14.4.7 Managing Disposition Tasks

The following tasks are performed when processing disposition actions:

- Screening for Retention Steps
- Viewing Failed Dispositions
- Viewing Pending Reviews and Dispositions
- Marking Content Items as Reviewed
- Editing Review Information

14.4.7.1 Screening for Retention Steps

> **Note:**
>
> The Admin.Audit right is required to perform this action. This right is assigned by default to the Records Administrator role.

To screen for disposition actions and events:

1. Choose **Records** then **Audit** then **Retention Steps** from the top menu.
2. On the Retention Step Search page, select the criteria for the search from the provided lists. The options on the lists will vary depending on customizations in place at the site. This list provides some examples of the type of criteria available:
   - Sources: Choose the repository source for the search. Click **Select** to display a list of sources that can be used.
   - Disposition Criteria: Includes criteria specific to dispositions such as a derived triggering event or location type.
   - Category Criteria: Includes criteria specific to retention categories such as restrictions (edits, revisions, deletions) and review information (review periods and reviewers).
   - Records Folder Criteria: Includes criteria specific to folders such as cutoff date, profile trigger, and freeze name for freezes applied to the folder.
   - Content Criteria: Includes criteria used for content such as author and content type.
   - Retention Steps Criteria: Includes options for retention actions such as freezing dispositions and action state.
3. Select sorting preferences in the **Results Options** area.
   - Use the defaults or select another option from the **Sort By** list.
   - Sort by default descending order or select ascending order.
4. To view the results of the screening immediately, click **Search**. Any results matching the screening criteria display in a result page.
5. To schedule the retention report to run later, select the criteria for the screening and click **Schedule**.
6. On the Schedule Retention Step Audit Report page, provide a name for the screening report.
7. Provide the start date of the screening report. This is the date the scheduled screening report will be generated. If the screening report is recurring, the first screening report is generated for the first time on this date, and all subsequent reports at the end of each recurring period after this date.
8. To create a screening report periodically rather than just once, select **Is Recurring**. Specify the interval at which the recurring screening report will be created (for example, every 2 weeks).
9. Click **OK** when done.

14.4.7.2 Viewing Failed Dispositions

> **Note:**
>
> The Admin.Audit right is required to perform this action. This right is assigned by default to the Records Administrator role.

If content is managed on an adapter system, no warning is given if the disposition will fail. If the disposition does fail, the action appears on the Failed Dispositions page. Check that page to verify the status of an adapter disposition. To find unsuccessful disposition actions:

1. Choose **Records** then **Audit** then **Failed Dispositions** from the top menu.
2. Use the Failed Dispositions page to view information about failed disposition actions. The following actions can also be performed:
   - To restart the disposition, select the check box for the item and choose **Retry** from the table menu.
   - To create a report of failed dispositions, select the items to include in the report then choose **Create Reports** from the table menu.
   - To mark the disposition as complete regardless of whether the action succeeded or not, select the check box for the item and choose **Skip** from the table menu. Use this option with caution because it may have unforeseen consequences when a disposition is skipped.

14.4.7.3 Viewing Pending Reviews and Dispositions

> **Note:**
>
> The Folder.Read right and Record.Read right are required to perform this action. All predefined management roles have this right. The Admin.PerformActions right is required to view your own or pending events of others. This right is assigned by default to the Records Administrator role.

To view pending actions to be taken:

1. Choose **Records** then **Approval** from the top menu.
2. Choose the type of pending approval to view: Reviews or Dispositions.
3. The resulting pages list actions awaiting approval. It lists actions assigned to the logged-in user as well as actions assigned to other users if the logged-in user has permission to see those actions.

14.4.7.4 Marking Content Items as Reviewed

> **Note:**
>
> The Admin.PerformPendingReviews right is required to perform this action. This right is assigned by default to the Records Officer and Records Administrator role. When performing reviews of items assigned to others, you must also be designated as the main notification recipient.

To review items that have been marked as Subject to Review, or items in a category that has a disposition that is Subject to Review:

1. Follow the link in the email sent by the system to notify the reviewer, or choose **Records** then **Approvals** then **Pending Reviews**.
2. On the Pending Reviews page, select the check box of the item to be reviewed then choose **Set Dates** and **Mark Reviewed** from the table menu. If this is a folder to review, the option **Mark Reviewed Recursive** can be used to mark all items in the folder as reviewed.

   In addition, you can choose **Set Dates** then **Mark reviewed** from the **Actions** menu for individual items.

   To perform a different action involving dates (mark the item as expired, cancelled, or obsolete, for example), choose **Set Dates** from the item's **Actions** menu and choose the appropriate menu option.
3. Enter a comment for the action (review, expiration, and so on) or leave that field blank if a comment is not needed.

   The current date is inserted to indicate the date when the action happened. This date can be changed by typing a new date or selecting one from the calendar icon.
4. After inserting the information, click **OK**.

   The item is removed from the list of pending reviews.

14.4.7.5 Editing Review Information

> **Note:**
>
> The Category.EditReview right or Folder.EditReview right is required to perform these actions. This right is assigned by default to the Records Administrator role.

To edit retention category or record folder review information:

1. Find the Retention category or folder to use.
2. Choose **Edit** then **Edit Review** from the page **Actions** menu (if editing a category review) or the item's **Actions** menu (if editing a folder review).

3. To change a review category to non-review category, deselect **Subject to Review**. The remaining fields become gray and unavailable. To change a non-review category to a review category, select **Subject to Review**.

> **Note:**
>
> The review setting is inherited. If items or record folders should stay as subject to review, set the review information for the child record folders that no longer inherit review status from their retention category. Any content filed directly into retention categories are directly affected by review status changes.

4. To select, remove, or change a reviewer, select the reviewer from the Reviewer list. Select the topmost blank to remove the reviewer and allow the system default to designate the reviewer.
5. To edit or enter the review period, enter an integer and select a review period in the **Review Period** box and list.
6. Click **Submit Update**.

   An update message appears, and the Retention Category Information page opens with the review information that was entered.

When editing folder review information, keep the following points in mind:

- The Folder.EditReview right is required to perform the action. This right is assigned by default to the Records Administrator role.
- Follow the same procedure to change folder review information as that used to change an item's review information. The review setting is inherited, and if any child folders should stay as subject to review, set the review information for record folders that no longer inherit it from a parent folder or category.
- The selected reviewer must have the Records Administrator or Records Officer role because users assigned the Records User role cannot mark a record folder as reviewed.

14.4.8 Pending Event Processing

Pending processing is accessed by choosing **Records** then **Approvals** and choosing **Pending Review** or **Pending Disposition**, or by clicking the link in the email notifying a user of dispositions or reviews to be performed.

Events for yourself are listed. To view assignments to other users, you must be added to the RmaReviewers alias. Then choose **List All** on the table menu on the Pending Dispositions page or Pending Reviews page.

The following list describes common functionality regardless of the type of action being processed:

- The Admin.PerformActions right is required to perform these actions. This right is assigned by default to the Records Administrator role.
- For most events, when the disposition event is processed, an audit log file is created automatically. A screening can be done for that audit log and it can be checked in as a content item if needed. An audit log is not created for a *Move* event or a *No Action* event.
- Most actions are run automatically with the batch services that are run nightly or when a Batch Services option is selected by choosing **Records** then **Batch Services**.

The pending events appear in both the other notification recipient's approval list and the filer's own approval list. If the main recipient processes the event, the event is removed from the author's approval list and vice versa. Some events only require approval. After approval of these events, their associated disposition actions are executed when the dispositions are run, usually nightly, unless otherwise processed by selecting an option from the **Batch Services** menu. The processed events are subsequently removed from the approval list.

Some events require multiple steps, depending on the event type and the item to be processed. First, they must be approved and after approval they must be marked as completed. Items marked as completed often must be physically moved to complete the action (for example, transferring an item to different location).

When an event must be marked as complete, it still appears on the Pending Dispositions page and the name of the event is changed to indicate it must be marked complete (for example, **Mark Transfer Complete**). To mark the item as complete, select the box for the item then choose **Approve** from the table menu.

To mark multiple items as reviewed, select the check box for the item and choose **Mark Reviewed** from the **Set Dates** menu on the Pending Reviews page. A prompt appears to enter any review comments.

The current date is inserted as the review date. This date can be changed by typing a new date or selecting one from the calendar icon.

After inserting the review information, click **OK**. The item is then removed from the list of pending reviews.

14.4.9 Processing Dispositions

Disposition actions can be divided into two types: those requiring one step for completion and those requiring multiple steps. This section describes each type of disposition processing.

Dispositions are grouped and held in batches. They are automatically scheduled and executed at the same time as other batch processes, normally at midnight or later.

To execute dispositions immediately, choose **Records** then **Batch Services** from the top menu. Select the type of action to process (dispositions, review, notifications, and so on).

If a processed event does not become available to mark as complete, then affected items (for example, content in a folder) are frozen and cannot be processed. Use the **List Disposition Folders and Content** option from the item's **Actions** menu to view the contents of the folder. The frozen items will not be processed until they are unfrozen. It is also possible the disposition failed. For information about checking on a disposition status, see Viewing Failed Dispositions.

This section describes the following types of dispositions:

- Multi-Step Disposition Processing
- Single Step Disposition Processing

14.4.9.1 Multi-Step Disposition Processing

The follow disposition events require multiple steps for processing:

- **Accession**: An accession is one of the last actions in a disposition sequence. Files for accession are stored in a directory (typically in the *weblayout_dir*/groups/secure/rm/RmaAccessionApp directory) and a user can then choose how to hand off the files to the final archive institution.

  The option also is available to destroy the items while retaining their metadata or to destroy items without retaining metadata. This option is selected when the category's disposition is created. An accession event consists of two steps: it must be approved first and then, after the action has been carried out, it must be marked as completed.

- **Archive**: The Archive action creates a zip file of the content and folder. Within each zip archive, there is a copy of each item and its metadata. The meta files contain the item metadata in the format specified by the Archive Meta Data Format setting on the Configure Retention Settings page (`hda`, `xml`, or `csv`). An archive event consists of two steps: it must be approved first and then, after the action has been carried out, it must be marked as completed. The `.zip` file is stored in a location on the computer. To see the location, choose **Archive Location** from the **Actions** menu of an Archive action on the Pending Dispositions page.

- **Move**: A move action does not leave a copy of internal (electronic) items on the system. This action should not be confused with moving retention items within the retention management system, which is accomplished with the **Move** command within the retention schedule (**Browse Content** menu). A move event consists of two steps: it must be approved first and then, after the action has been carried out, it must be marked as completed.

- **Transfer**: A transfer action leaves a copy of internal (electronic) items on the retention management system. A transfer event can be considered complete when an organization sends the items to another organization. A transfer event consists of two steps: it must be approved first and then, after the action has been carried out, it must be marked as completed. A *terminal transfer* action is when the transfer disposition action is the last action for a disposition schedule. If the Transfer action is the last step (rule) in a disposition action, the items must be destroyed before the step can be marked as completed.

One aspect of these events is the ability to destroy items in conjunction with the processing. For example, you can choose to transfer items and destroy the metadata after the transfer, or you can retain the metadata. Another example is to move content and either destroy or keep the metadata. These actions are chosen when the disposition for the category is set up initially.

The number of disk scrubbing passes that accomplish the destruction can be configured by setting the following variable in the `config.cfg` environment file:

```
RecordsManagementNumberOverwriteOnDelete
```

Restart Content Server after setting this variable. By default, the number of scrubbing passes on the hard disk is set to 2.

The destroy process can consist of one or two steps. For electronic (internal) items, multiple actions are carried out automatically by the system. If metadata was to be destroyed with the items, that is done as well.

For physical (external) items, which are managed using Physical Content Management, two steps are required: the event must be approved first and then, after the external items have been destroyed manually, it must be marked as completed.

Approval Step

The name listed in the ID column is the name of the category involved in the disposition followed by a step number. Numbering begins with step 0.

1. Choose **Records** then **Approvals** from the top menu.
2. Choose **Pending Dispositions** or click the link in the notification email.
3. To view information about the disposition action, click the action name on the Pending Dispositions page. The Disposition Information page opens. To view what items are included in this action, choose **List Disposition Folders and Content** from the **Actions** menu of a disposition action. An individual disposition can also be approved from this menu.
4. Select the check boxes of the actions to approve and choose **Approve** from the table menu.
5. In the Disposition Parameter dialog, enter a reason for the action and click **OK**. To abort the entire action, click **Cancel**.
6. The action is approved. After processing (either during the scheduled processing time or after a batch service is run) the event appears on the Pending Dispositions page and is available to mark as completed if needed.

Completion Step

After an item has been marked as approved and is processed, it remains on the Pending Dispositions page but the name of the action is changed to **Mark** *action* **Complete** (for example, `Mark Accession Complete`).

Internal items are completed as needed automatically. This action is transparent to users but the system approval steps are listed in the disposition.

To mark an action as completed:

1. Choose **Records** then **Approvals** from the top menu.
2. Choose **Pending Dispositions** or click the link in the notification email.
3. To view information about the disposition action, click the action name on the Pending Dispositions page. The Disposition Information page opens. To view what items are included in this action, choose **List Disposition Folders and Content** from the **Actions** menu of a disposition action. An individual disposition can also be approved from this menu.
4. Select the check boxes of the actions to approve (mark complete) and choose **Approve** from the table menu.
5. On the Disposition Parameter dialog, enter a reason for the disposition action and click **OK**. Click **Cancel** to abort the entire action.

   If the action requires a decision involving destruction (that is, to destroy or keep metadata associated with the action), choose a destruction method from the menu in the Disposition Parameter dialog. Disposition actions that involve such a choice are Accession, Archive, Move, and Transfer.
6. The action is removed from the Pending Dispositions page. If further approvals are needed (that is, if another action must be taken to complete the disposition) that action will appear on the Pending Dispositions page after processing (either during the scheduled processing time or after a batch service is run.

14.4.9.2 Single Step Disposition Processing

The following dispositions require single step processing:

- **Classified Records Actions**
  - **Review Classification**: This action indicates it is time to review the security classification status of an item.
  - **Upgrade Classification**: This action indicates it is time to increase the security classification of an item. Classifications can be increased as high as the classification of the user applying the classification.
  - **Declassify**: This action indicates it is time to declassify content.
  - **Downgrade Classification**: This action indicates it is time to lower the security classification of an item.
- **Dispose Actions**
  - **Delete Previous Revision**: This action indicates it is time to delete the revision before the content item revision that triggered the disposition action. The revision that activated the trigger may be the latest revision of a content item, but does not need to be.
    - If a content item has 5 revisions and this disposition action is activated for revision 5 (the latest revision), then only revision 4 is marked for deletion.
    - If a content item has 5 revisions and this disposition action is activated for revision 3, then only revision 2 is marked for deletion.
  - **Delete Revision**: This action indicates it is time to delete the content item revision that triggered the disposition action. This revision may be the latest revision of a content item, but does not need to be.
    - If a content item has 5 revisions and this disposition action is activated for revision 5 (the latest revision), then only revision 5 is marked for deletion.
    - If a content item has 5 revisions and this disposition action is activated for revision 3, then only revision 3 is marked for deletion.
  - **Approve Deletion**: This action indicates it is time to approve record folders or content for deletion.
  - **Delete All Revisions**: This action indicates it is time to delete the content item revision that triggered the disposition action and all earlier revisions. The revision that activated the trigger may be the latest revision of a content item, but does not need to be.
    - If a content item has 5 revisions and this disposition action is activated for revision 5 (the latest revision), then revisions 1 through 5 are marked for deletion (effectively removing the content item altogether).
    - If a content item has 5 revisions and this disposition action is activated for revision 3, then revisions 1 through 3 are marked for deletion.
    - If the DoD Config module is enabled, all revisions can be deleted and the metadata destroyed or kept, or only old revisions destroyed. Metadata cannot be retained unless the DoD Config module is enabled.
  - **Delete Old Revisions**: This action indicates it is time to delete all revisions before the content item revision that triggered the disposition action. The revision that

activated the trigger may be the latest revision of a content item, but does not need to be.

  * If a content item has 5 revisions and this disposition action is activated for revision 3, then revisions 1 and 2 are marked for deletion.
  * If a content item has 5 revisions and this disposition action is activated for revision 5 (the latest revision), then revisions 1 through 4 are marked for deletion.

- **Delete Working Copy**: This action deletes the working copy of a cloned content item. It first deletes the direct working copy of the clone. Then all previous revisions of the working copy are deleted until a revision of the fixed clone itself is found. The deletions stop at that point.
- **Delete Previous Clones**: This action deletes the previous clone of a content item.

- **Other**
  - **Check in New Revision**: This action indicates it is time to take the latest revision of the affected content items and check in a copy of this revision as a new revision. This may be useful to process a content item revision based on changed historical information, refresh an expired document, or enter a content item into a criteria workflow for disposition processing.
  - **Activate**: This action indicates it is time to activate record folders or content.
  - **Close**: This action indicates it is time to close record folders.
  - **Cutoff**: This action indicates it is time to cut off content or record folders from further processing. Cutoff refers to changing the status of items to prohibit further processing.
  - **Cutoff and Create Volume**: This creates a volume folder, content is placed inside, and the volume is cut off.
  - **Expire**: This action indicates it is time to expire record folders or content.
  - **Obsolete**: This action indicates it is time to mark content as obsolete.
  - **Mark Related Content**: This action marks any content linked to the current content. This can be used as a trigger action in a custom direct trigger that uses the `xRelatedContentTriggerDate` field.
  - **No Action**: This action indicates there is no action to take currently. This action is usually found mid-disposition. A No Action action acknowledges a disposition milestone has passed, and the next step in the disposition begins processing.
  - **Notify Authors**: This action indicates it is time to notify the author of the affected category that disposition actions are due for the category.
  - **Supersede**: This action indicates that new content will be checked into the category or folder, superseding the original content item. The superseded item is indicated by a strikethrough on its name.

Approving Events

1. Choose **Records** then **Approvals** from the top menu.
2. Choose **Pending Dispositions** or click the link in the notification email.

3. On the Pending Dispositions page, click the action name to view information about the disposition action.

   The Disposition Information page opens.

4. To view what items are included in this action, choose **List Disposition Folders and Content** from the **Actions** menu of a disposition action. Individual items affected by the current action can also be approved using this menu.

5. Select the check boxes of the actions to approve and choose **Approve** from the table menu.

6. In the Disposition Parameter dialog, enter a reason for the action and click **OK**. To abort the entire action, click **Cancel**.

   The action is approved and is removed from the Pending Dispositions page.

15

Managing the Oracle WebCenter Content Records Adapter

This chapter discusses how to configure and use the Oracle WebCenter Content Server Adapter to provide a bridge between the Oracle WebCenter Content: Records system (which contains the record management policies) and an adapter server's content vault (which stores additional content). Corporations can then manage records, retention policies, and legal holds across multiple systems from a single location.
An adapter sends information back to the Records server so it can maintain an up-to-date catalog of the enterprise's important content. By doing so, companies can apply their records and retention policies to more content, more consistently, with less administrative effort and less disruption for users. These same benefits apply to litigation searches and holds. The Record Adapter for Content Server (hereafter abbreviated as the Content Server Adapter) obtains these policies from the server and applies them to the content items stored in the vault.

Multiple adapters can be used with the Records system to manage an enterprise's content needs. This chapter discusses how to configure and use one specific adapter, the Content Server Adapter.

This chapter contains the following topics:

15.1 Understanding the Content Server Adapter

The major components involved in a typical Content Server Adapter installation include:

- Records system: Enables organizations to manage their content and retention policies, disposition processes and litigation or audit holds in a central repository. These policies, dispositions, and holds can then be applied to external repository content through the Content Server Adapter.
- Oracle WebCenter Content: Stores and manages content in a repository.
- Adapter: Communicates between Records and the Content Server Adapter's content vault. The Content Server Adapter provides common retention functionality as follows:
  - Identifying the content in the repository that is of interest to the Records system.
  - Performing searches and declaring the applicable content items to the Records system.
  - Performing disposition actions on the existing content items when their retention periods end.
  - Establishing and removing holds and freezes on the content items, as necessary.

The Records system manages records and retention policies, disposition processes, and litigation holds or freezes in a central repository. Those policies, dispositions, and holds can

be applied to content stored in multiple repositories by using adapters. The repositories may be any server or application that holds content whose retention is to be controlled.

The Content Server Adapter server's content vault holds content that must be preserved for a retention period, specified in a corporate retention schedule, and then destroyed according to a corporate disposition process. The records are preserved in place because the Content Server Adapter ensures that the record remains unalterable during the retention period. Upon request, the Content Server Adapter vault can purge the content at the end of the retention period.

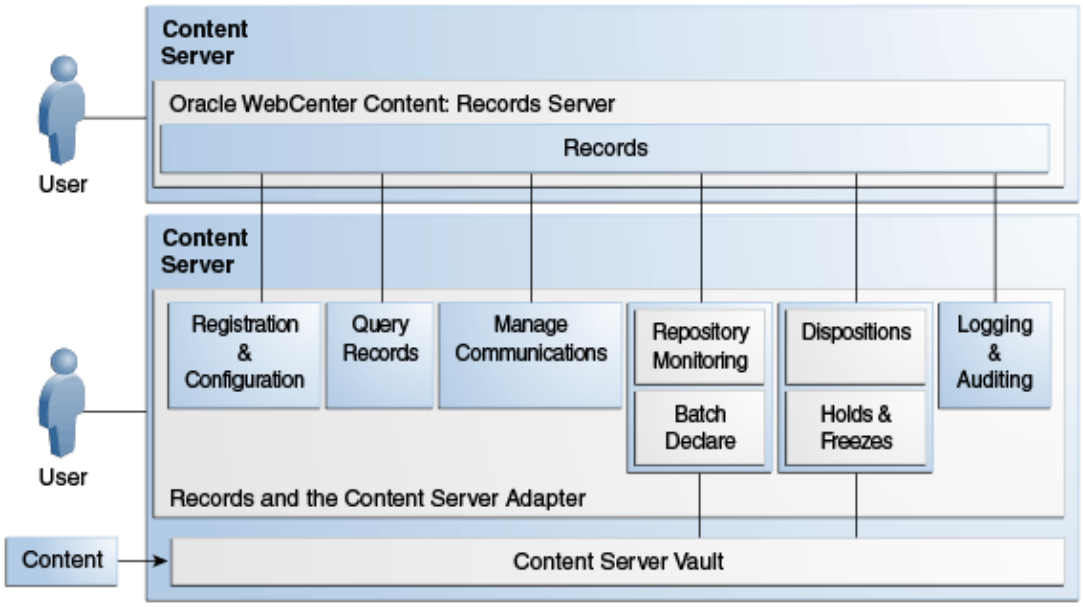
The Content Server Adapter vault may also hold content that does not need to be retained. When retention of this content is no longer necessary, it can be disposed of according to the disposition processes stored within the Records system.

There is an obligation to ensure that any material that is subject to a litigation or audit hold (freeze) is not deleted, either by a user or as part of a disposition process. The Content Server Adapter enables the Records system to ensure deletions do not happen.

> **Note:**
>
> Content items that are non-records and are not subject to a litigation or audit hold are not transferred to the Records system. Instead, these documents remain in the Content Server Adapter vault and only their metadata is stored in the Records system.

The Content Server Adapter is the communications intermediary between the Records system and the Content Server Adapter repository. Content is stored in and remains in the Content Server Adapter vault while the Records system simultaneously enforces corporate retention policies, disposition processes, and legal holds on the stored content.

Figure 15-1 Content Server Adapter Retention Functions Overview



The Content Server Adapter can be configured to provide the following basic retention functions:

- Registration: The Content Server Adapter self-registers with the Records system, ensuring that the Records system knows about the Content Server Adapter vault and is thus ready to manage the stored content within the repository.
- Configuration: Content Server Adapter configuration includes collecting the proper identification and credentials information for the Records system security and communications. Configuration information also includes mapping metadata fields and defining synchronization schedules.
- Query the Records System: The Content Server Adapter queries the Records system for certain information. For example, it may need to retrieve retention schedules for specific items of interest. Or the Content Server Adapter may need to request Records metadata for content items and obtain life cycle information.
- Manage Communications: The Content Server Adapter monitors batch processes, handles communication errors with the Records system, and handles large work requests by grouping them into communication blocks and processing the response in chunks.
- Repository Monitoring and Batch Declare: The Content Server Adapter monitors its server's content vault by periodically searching the repository and informing the Records system of any changes in the repository that may affect disposition processes or audit holds. For example, the Content Server Adapter will inform the Records system about new content checkins that need to be managed.
- Perform Records Tasks: The Content Server Adapter periodically checks the Records system for tasks to be performed within the repository. These tasks enable the Records system to abide by the corporate retention policies and disposition processes. Typical tasks include:
  - The Records system may use the Content Server Adapter to perform a search within the Content Server Adapter vault and provide a list of items matching the search criteria.

  - When a litigation hold applies to managed content within the Content Server Adapter vault, the Records system may use the Content Server Adapter to retrieve a list of affected items and preserve them to ensure that they are not edited or destroyed.
  - When a litigation hold is removed, the Content Server Adapter can be used to stop preserving the affected items and dispose of them according to retention schedule rules and instructions.
- Logging and Auditing: The Content Server Adapter provides consistent logging for the activities it coordinates. It contributes event information to the log files that are then uploaded to the Records system, consolidated, and stored.

15.2 Adapter Configuration

The initial step in setting up the Content Server Adapter is to access the **Administration** menu on the remote server where the adapter will reside. Choose **Administration** then **Configure Record Settings** then **Adapter**. Select the Adapter option.

When the Adapter option is chosen on the Configure Retention Settings page on a remote repository, the necessary component software is enabled. The system must then be restarted in order for the installation to be complete.

Next define an outgoing provider on the Adapter's server and register the repository source. The documents in that repository are managed using the Records system retention policies.

After registration of the source, a check is automatically made to compare content on the Content Server Adapter and the Records system repository. A list is presented of items that do not match. At that time the items on the Content Server Adapter repository can be deleted so the two systems are in sync.

Next metadata fields should be mapped. The Content Server Adapter repository may contain a wide variety of documents and may have custom fields that do not directly correlate to those on the Records system repository. When adapter documents are classified into groups, there can be a wide variety of retention categories associated with the content. The metadata fields between the two repositories must be mapped so the content is categorized correctly.

The Content Server Adapter does not synchronize security groups with the Records system. When using the Imaging functionality with the Adapter the security groups do not match if data is later synchronized with the Records system. The Imaging system creates new security groups dynamically, as needed for applications. Therefore, plan to set up the same security groups on the Imaging system and the Content Server Adapter that are used on the Records system.

The Access Control List (ACL) settings are also not synchronized between the Content Server Adapter and the Records system. This means that it is possible to have a higher ACL security setting on one system than on the other, or to have ACLs disabled on one system. The administrators for the systems should ensure that ACLs are set appropriately for the site's needs.

For complete details about defining and using providers, see *Administering Oracle WebCenter Content*.

> **Note:**
>
> Revisioning of external items differs from revision of items stored on Oracle WebCenter Content. For example, if an item is created on the adapter system and is synchronized to the Records system, it appears as a single item. However, if that item is revised on the adapter system then synchronized to the Records system, the item now appears in the category as two items, not one item with two revisions. Both items have the same content ID, which is the default behavior for external items.

This section describes the basic tasks needed to configure and use the Content Server Adapter:

- Configuring Sources and Providers
- Managing Fields

15.2.1 Configuring Sources and Providers

Use these procedures to configure the source and provider.

- Defining a New Outgoing Provider
- Editing an Outgoing Provider
- Disabling the Adapter's Outgoing Provider
- Deleting the Adapter's Outgoing Provider
- Registering an External Source
- Unregistering and Removing an External Source

15.2.1.1 Defining a New Outgoing Provider

Use this process to define an outgoing provider:

1. Choose **Records** then **Record Adapter**.
2. Choose **Configure** then **Source Registration**.
3. On the Register Source page, click **Add**.
4. On the Add or Edit New Provider page, enter the required information in the appropriate fields:
   - **Provider Name**: The name of the outgoing provider. Special characters are not allowed.
   - **Provider Description**: A description of the provider.
   - **Server Host Name**: Host name of the instance on the Records system server.
   - **HTTP Server Address**: The URL of the instance.
   - **Server Port**: The port on which the provider communicates with the instance.
   - **Instance Name**: Name of the instance on the Records system server.
   - **Relative Web Root**: The relative root of the instance.

5. Click **Add** when done.

To use a 10*g* adapter with Records 11*g*, a connection string must be changed. Previous connection strings were similar to the following example:

```
http://myhost.mycompany.com:myport/URMinstance/idcplg
```

The new connection string should be similar to the following example:

```
http://myhost.mycompany.com:myport/_dav/URMinstance/idcplg
```

The addition of the `_dav` string is all that changes. The `_dav` string forces Content Server to use basic authentication instead of form-based authentication.

15.2.1.2 Editing an Outgoing Provider

Use this process to define an outgoing provider:

> **Note:**
>
> The Adapter does not allow you to edit the outgoing provider if it is linked to an external Records source. You must first undo this link before editing the outgoing provider.

1. Choose **Administration** then **Providers**.
2. On the Provider List page, navigate to the provider to edit and click **Info**.
3. On the Provider Information page, click **Edit**.
4. Edit the information as needed and when done, click **Save**.

15.2.1.3 Disabling the Adapter's Outgoing Provider

To disable an existing outgoing provider on the Adapter server:

1. Choose **Administration** then **Providers**.
2. On the Provider List page, navigate to the provider to disable and click **Info**.
3. On the Provider Information page, click **Disable**.
4. A prompt appears to confirm the choice. Click **OK**.

   The outgoing provider is disabled.

15.2.1.4 Deleting the Adapter's Outgoing Provider

To delete an existing outgoing provider on the Adapter server:

> **Note:**
>
> The Adapter does not allow you to delete the outgoing provider if it is linked to an external Records source. You must first undo this link before deleting the outgoing provider.

1. Choose **Administration** then **Providers**.
2. On the Provider List page, navigate to the provider to delete and click **Info**.
3. On the Provider Information page, click **Delete**.

   A prompt appears to confirm the choice.
4. Click **OK**.

   The outgoing provider is removed from the Providers table.

15.2.1.5 Registering an External Source

Only one source per adapter can be registered.

To register an external source:

1. Choose **Records** then **Record Adapter**.
2. Choose **Configure** then **Source Registration**.
3. On the Register Source page, enter the required information in the appropriate fields:
   - **Provider Name**: Name of the outgoing provider that was configured for communication between the Adapter server and the Records system server.
   - **Source Name**: Name of the Records system source to be created on the Records system server.
   - **Source Display Name**: Name used in the user interface to identify the source.
   - **Source Table Name**: Prefix of the database tables created for the source.
4. Click **Register** when done. Registration ensures that the Records system is aware of the Adapter and is ready to manage the stored content in the Adapter server's repository.

15.2.1.6 Unregistering and Removing an External Source

> **Note:**
>
> Unregistering a source clears the data on the external source. You should export and archive the data before unregistering a source.

To unregister an external source:

1. Choose **Records** then **Record Adapter** then **Unregister Source**.
2. A prompt appears to confirm the action. Click **OK** to continue.

Follow this procedure to remove an external source and the database tables associated with the source.

> **Note:**
>
> If you remove an external source, you must reconfigure the external source in order to use it again.

1. Choose **Records** then **Configure**.
2. Choose **Retention** then **Remove External Sources**.
3. Highlight the name of a source to remove and click **Remove** or click **Reset** to clear the highlighting. To remove multiple items, hold down the shift key and highlight multiple items.
4. To delete the database tables associated with the source(s), select **Delete External Source Database Tables**.

   All database tables associated with the external source are deleted.

15.2.2 Managing Fields

Fields on the Adapter's remote source must be mapped to fields already in use on the Records system local source. If fields do not exist that match those on the Adapter, create a custom metadata field to accommodate the Adapter data.

15.2.2.1 Mapping a Custom Field to a Remote Source

To map a custom metadata field to a remote source:

1. Choose **Records** then **Record Adapter**.
2. Choose **Configure** then **Custom Fields**.
3. On the Map Custom Fields page, click **Add**.
4. A list of custom metadata from the remote source is available in a list. Select a metadata field for use from the list on the Map/Edit Custom Field dialog and enter a name and caption for that field to be stored in the Records system database table. You can also enter a different name. If entering a new name, the Adapter automatically creates a corresponding custom metadata field for the name.
5. Click **OK**.

   The custom metadata field is added to the list of custom metadata fields on the Map Custom Fields page.
6. To change the field order, use the **Up** or **Down** arrow keys to move the position of the field.

15.2.2.2 Editing a Mapped Field

To edit a previously mapped field:

1. Choose **Records** then **Record Adapter**.
2. Choose **Configure** then **Custom Fields**.
3. On the Map Custom Fields page, select a metadata field from the list, and click **Edit**.
4. On the Map/Edit Custom Field dialog, alter information as needed and click **Update**.
5. To change the field order on the Map Custom Fields page, use the Up or Down arrow keys to move the position of the field.

15.3 Synchronizing Data

After configuring the Adapter for use with the Records system, determine a synchronization schedule to ensure that content on both systems, the Adapter and the Records system, are consistently synchronized. This section describes the tasks involved in establishing synchronization.

The systems can also be synchronized on an as-needed basis by selecting an option from the Content Server Adapter menu. These operations synchronize all items involved in the operation. For example, all content involved in freeze events are synchronized. Individual freeze events cannot be selected to be synchronized.

> **Note:**
>
> Revisioning of external items differs from revision of items stored on Oracle WebCenter Content. For example, if an item is created on the adapter system and is synchronized to the Records system, it appears as a single item. However, if that item is revised on the adapter system then synchronized to the Records system, the item now appears in the category as two items, not one item with two revisions. Both items have the same content ID, which is the default behavior for external items.

The following options can be synchronized:

- Retention Schedule: synchronizes the entire retention schedule between the two systems.
- Content: Choose from the following types of synchronization operations:
  - Upload: Find and synchronize recently uploaded content.
  - Delete: Find and synchronize newly deleted items.
  - Freeze: Find and synchronize items that have been frozen or unfrozen.
- Content Dates: Synchronizes any date field that has changed. If both the external source and the local repository have different dates, the earliest date is used regardless of whether it is on the Adapter or the Records system repository.
- Mark Complete: Synchronizes items that are ready for approval and completion of disposition processing.
- Upload Archives: Synchronizes uploaded archives.
- Mark Vital: Synchronizes items marked for vital review.
- All: synchronizes all possible operations.

The following sections discuss synchronization:

- Performing As-Needed Synchronization
- Scheduling Synchronization
- Viewing Synchronization Logs

15.3.1 Performing As-Needed Synchronization

Follow this procedure to synchronize content based on specific synchronization operations:

1. Choose **Records** then **Record Adapter**.
2. Choose **Synchronize** then click the type of synchronization to perform. The operation is performed.
3. If the operation completes successfully, a message is displayed. Click **OK** to continue.
4. If an error occurs, a message is displayed. Check the synchronization logs to view the details of the operation and which items may have failed synchronization. For details, see Viewing Synchronization Logs.

15.3.2 Scheduling Synchronization

Follow this procedure to set up a schedule to perform regular synchronization:

1. To access this page, choose **Records** then **Record Adapter**.
2. Choose **Configure** then **Scheduled Events**.
3. On the Configure Scheduled Events page, choose the unit of time measurement from the list and the amount of time to elapse between synchronizations.
4. Choose a time for synchronization that will not affect system performance.
5. When done, click **Save**.

15.3.3 Viewing Synchronization Logs

Follow this procedure to view logs that are automatically generated during any synchronization activity, either on-demand or scheduled.

1. Choose **Records** then **Record Adapter**.
2. Choose **Logs** then choose the type of log file to view.
3. On the Synchronization Log page, to view additional details about the logged event, choose **View Items** from the operation's **Actions** menu.
4. To rerun the operation, choose **Rerun Task** from the operation's **Actions** menu.

16
Managing Physical Content

This chapter describes the tasks involved in configuring and managing physical records and content that are not stored in the repository in electronic form. This functionality is only available if the Physical Content Management feature has been enabled. It is enabled by default for all levels except the Minimal level.
This chapter covers the following topics:

16.1 Configuring Physical Content Management

Physical Content Management (PCM) is used to manage physical records and content that are not stored in the repository in electronic form (for example, physical media such as compact disks). All items, both internal and external, regardless of their source or format are managed using a single user interface. The same retention schedule can be used for both electronic (internal) and physical (external) content.

Storage location and retention schedules of the physical items can be tracked. This is done by using several key features:

- **Space management**: Defines how items are stored, from the largest storage area (warehouse layouts) to fine details (cases, shelves, bins).
- **Circulation services**: Sets up reservations for handling requests for items, checking them out to users and tracking the space used and available space.
- **Chargeback services**: Defines costs for storage services or other actions performed on physical items. These costs can then be invoiced to defined customers.
- **Barcode processing**: Defines barcodes for customers and for storage locations, enabling quick processing of reservations, storage, and invoicing information. Barcode data can be uploaded automatically into PCM or can be entered manually.
- **Label creation and printing**: In conjunction with barcodes, this is used to create barcode labels for items, storage, and customers.
- **Retention management**: Sets up retention schedules for external items and freezes them, sends email for pending events, or performs periodic reviews of storage and items.

In addition to storing items locally, offsite storage capabilities can be set up to move archive content to a different location.

> **Important:**
>
> Content server is specifically designed to take advantage of the Oracle Text Search full text search capability. This involves indexing both the content and the metadata and putting it in the Oracle Text Search full text search engine. When doing this, Oracle Text Search provides case insensitive search. However, physical content does not have a file and the metadata for physical content resides in a different location from the internal content. Therefore, physical content search is not case insensitive.

The following list in Table 16-1 describes the tasks needed to set up a PCM environment.

Table 16-1 Tasks to Set Up a PCM Environment

Task	Description
Establish the required user roles and rights	Determine and configure the user roles and rights required for the PCM environment.
Configure chargeback processing	Define payment types (credit, cash, and so on), charge types (billable events), and customers (organizations or users who are billed for services).
Configure location types	Define the locations that hold physical content. Location types can include warehouses, rooms, bays, shelves, and other storage areas.
Configure object types	Define the kinds of items stored in the locations. A storage location can hold a specific kind of object, and if a user attempts to store an object in an incorrect location, an error occurs.
Configure media types	Define what kinds of media are associated with objects. For example, optical is a type of object and it can have several different media types such as mixed, CD, Disc, or DVD.
Configure default reservation information	Default metadata values can be set for reservations and for items that are stored offsite.
Create barcode labels for content, storage and users	Default values are provided for users but barcode labels can also be designed.
Define your storage space environment	After defining location, object, and media types, assign relationships in the storage space to those types.
Create disposition rules for physical content (if required)	This is similar to creating rules for non-physical content.

This section discusses the following topics:

- Configuring Chargeback Processing
- Configuring Location Types
- Configuring Object Types
- Configuring Media Types
- Configuring Default Metadata Values: Offsite and Reservations

16.1.1 Configuring Chargeback Processing

Chargebacks are fees charged to people or businesses for the use of storage facilities or actions performed on physical items in the storage facilities. PCM can be used to generate invoices for the storage, use, reservation, and destruction of the managed content. These invoices can then be sent to the internal or external customers in accordance with the applicable business procedures.

Depending on rights and roles assigned, users or administrators can set up chargebacks and customers. For details about configuring chargebacks and customers, see *Using Oracle WebCenter Content*.

16.1.2 Configuring Location Types

> **Note:**
>
> The PCM.Admin.Manager right is required to set up location types. This right is assigned by default to the PCM Administrator role.

Location types are used in the definition of the storage space holding the physical content. They represent the hierarchy of storage units where items can be stored. PCM uses the location types and their defined hierarchy to keep track of the locations of the managed external physical content. Reordering location types does not affect any existing storage locations. The following topics are discussed in this section:

- Predefined Location Types
- Location Type Icons
- Creating or Editing a Location Type
- Viewing Location Type Information
- Deleting a Location Type
- Reordering Location Types
- Example: Creating a Location Type

16.1.2.1 Predefined Location Types

The default Physical Content Management functionality comes with the following six predefined location types (in hierarchical order), with their standard icons for the default Trays layout.

Predefined Location Types	Icon (large)	Allows Storage of Content (Default)
Warehouse		No
Room		No
Row		No
Bay		No
Shelf		No
Position		Yes

These are the default settings, which can be modified. Storage of content applies to a particular level only, not to any lower levels. For example, in the default hierarchy shelves have several positions, each of which can hold content items, but no content items can be directly assigned to the shelf level (only to the positions on a shelf). The location type 'Shelf' cannot store content, whereas the type 'Position' can.

These predefined location types are hierarchical. A warehouse consists of one or more rooms, a room consists of one or more rows, a row consists of one or more bays, and so on.

16.1.2.2 Location Type Icons

Each defined location type can be assigned an icon used to indicate the location type of storage locations. The icons are located in `/weblayout/ resources/layouts/`*`Layout_Name`*`/`*`Skin_Name`*`/Pcm_Icons`, and come in three varieties:

- *`Name`*`_lg.gif`: This is the large variety of the icon (32x32 pixels), used in the thumbnail view of the exploring pages.
- *`Name`*`_sm_closed.gif`: This is the small variety of the icon (16x16 pixels) used to indicate the location types of storage locations in the storage space tree view. This appears in the Trays layout when the child tree below the storage location is collapsed or when there are no child storage locations.
- *`Name`*`_sm_open.gif`: This is the small variety of the icon (16x16 pixels) used to indicate the location types of storage locations in the storage space hierarchy when the child tree below the storage location is opened.

The open and closed icons for the predefined location types are identical, but they can be changed.

Customized icon files can be added to the image selection list for location types by copying three `gif` files with the above naming pattern) for each icon to the appropriate `Pcm_Icons` directories. For example, you could create icon files called `Storage_archive_lg.gif` (32x32 pixels), `Storage_archive_sm_open.gif` (16x16 pixels), and `Storage_archive_sm_closed.gif` (16x16 pixels), and copy these to the previously mentioned directory to make them available in the default Trays layout.

If icons were created in a previous version of this software they are not automatically transferred during an upgrade. They must be copied after upgrading.

16.1.2.3 Creating or Editing a Location Type

> **Note:**
>
> The `PCM.Admin.Manager` right and the `PCM.Admin.LocationTypes` right are needed to perform this action. These rights are assigned by default to the PCM Administrator role.

The following information is a general navigational procedure. To view a specific example of creating a custom metadata field, see Example: Creating a Location Type.

1. Choose **Physical** then **Configure**.
2. Choose **Types** then **Location Types**.
3. Click **Add** on the Configure Location Types page.
4. On the Create or Edit Location Type page, specify the properties of the location type:
   - **Location Type ID**: An identifier for the location type displayed in the location type hierarchy. Maximum characters: 30.
   - **Location Name**: Name for the type. Maximum characters allowed: 30.
   - **Description**: A brief description of the type.

- **Tooltip**: Text that appears if the mouse cursor is held over the option in the location type selection list. Maximum characters: 30
- **Allow storage of content (default)**: Select to allow the location type to hold content items by default. This can be overridden when defining storage locations. Overriding the default setting may be useful to accommodate abnormal storage locations, or to create a dummy storage location that enables a user to maintain consistent numbering across parallel objects.

  This setting applies to this specific location type level only, not to any location types lower in the hierarchy. Therefore, the box for a location can be disabled if its child location types will contain content. For example, in the default hierarchy shelves have several positions, each of which can hold content items. But no content items can be directly assigned to the shelf level (only to the positions on a shelf). Therefore, the Shelf location type does not allow storage of content, whereas the Position location type does.
- **Maximum Items Allowed**: available only if **Allow storage of content (default)** is selected. This specifies the default maximum number of content items a location type can hold. This can be overridden when defining storage locations in the storage space hierarchy. This number applies to storage of content on this specific location type level only, not to any location types lower in the storage space hierarchy.
- **Image**: Specifies the icon to use for the location type.

5. Click **OK** when done.

   The new location type is now added to the bottom of the list on the Configure Location Types page. If required, click the **Up** and **Down** arrows to move the new location type to its new position in the location type hierarchy.

To modify a location type, select the type to edit in the list and choose **Edit** from the **Actions** menu. Modify the properties as required and click **OK** when finished.

16.1.2.4 Viewing Location Type Information

> **Note:**
>
> The PCM.Admin.Manager right and the PCM.Admin.LocationTypes right are needed to perform this action. These rights are assigned by default to the PCM Administrator role.

To view information about an existing location type:

1. Choose **Physical** then **Configure**.
2. Choose **Types** then **Location Types**.
3. On the Configure Location Types page, select the location type and click the **Info** icon.

   The information page opens.
4. When done viewing information, click **OK**.

16.1.2.5 Deleting a Location Type

> **Note:**
>
> The PCM.Admin.Manager right and the PCM.Admin.LocationTypes right are needed to perform this action. These rights are assigned by default to the PCM Administrator role.

To delete an existing location type but not delete the location:

1. Choose **Physical** then **Configure**.
2. Choose **Types** then **Location Types**.
3. On the Configure Location Types page, select the location type to delete and click **Info**.

   The information page opens.
4. Choose **Delete** from the page menu.

16.1.2.6 Reordering Location Types

> **Note:**
>
> The PCM.Admin.Manager right and the PCM.Admin.LocationTypes right are needed to perform this action. These rights are assigned by default to the PCM Administrator role.

To change the hierarchical order of the defined location types:

> **Note:**
>
> Reordering location types does not affect existing storage locations. You must remove the existing storage locations and rebuild the storage environment if you want it to match the reordered location types.

1. Choose **Physical** then **Configure**.
2. Choose **Types** then **Location Types**.
3. On the Configure Location Types page, use the **Up** and **Down** arrows to move location types to the new level in the hierarchy.
4. Repeat this step for every location type to move until the new storage hierarchy is achieved.
5. When finished, click **Submit Update**.

   A message appears stating the location types were configured successfully.

6. Click **OK** to return to the Configure Location Types page.

16.1.2.7 Example: Creating a Location Type

> **Note:**
>
> The PCM.Admin.Manager right and the PCM.Admin.LocationTypes right are needed to perform this example. These rights are assigned by default to the PCM Administrator role.

This example creates a location type called Box, located at the bottom level of the storage level hierarchy (below Position). Therefore, each position contains one or more boxes, each of which can contain a maximum of five physical content items.

1. Choose **Physical** then **Configure**.
2. Choose **Types** then **Location Types**.
3. Click **Add** on the Configure Location Types page.
4. In the **Location Type ID** field on the Create or Edit Location Type page, type `Archive`.
5. In the **Name** field, type `Box`.
6. In the **Description** field, type a description of the location type (optional).
7. In the **Tooltip** field, type a tooltip for the location type (optional).
8. Verify that **Allow storage of content (default)** is selected, and enter `5` in the **Content Items Allowed** field.
9. In the **Images** list, choose the `storage_box_lg.gif` icon image. This image is used to indicate the location type of storage locations in the Browse Storage tree in the Trays layout.
10. Click **OK**.

    A message appears stating the location type was created successfully, along with the properties of the newly created location type.
11. Click **OK**.

    The Configure Location Types page opens with the new location type Box added to the bottom of the list of location types.

16.1.3 Configuring Object Types

Object types define the types of items that storage locations can hold. When creating a physical item, specify its object type. If you select an object type that is not allowed for the assigned storage location, an error message is displayed and you cannot check in the physical item.

Object types can hold other object types. For example, the predefined Box object type can hold the following predefined object types: Folder, Optical, Micro, Document, and Tape. Relationships between object types are defined on the Edit Object Type Relationships page.

The following topics are discussed regarding object types:

- Predefined Object Types
- Creating or Editing an Object Type
- Viewing Object Type Information
- Deleting an Object Type
- Editing Object Type Relationships

16.1.3.1 Predefined Object Types

PCM comes with the following predefined object types:

- All (any of the predefined object types, including custom types). An All object type cannot be assigned to a physical item in this version of the software.
- Box
- Document
- Folder
- Micro
- Optical
- Tape

You can further specify what a storage location can hold using media types. For details, see Configuring Media Types.

You do not need to specify an object type when creating a storage location. The storage location can then hold any type of content. If you do select an object type, and you attempt to assign a physical item of a different object type to the storage location, an error message is displayed and you cannot check in the physical item.

16.1.3.2 Creating or Editing an Object Type

> **Note:**
>
> The PCM.Admin.Manager right is needed to perform this action. This right is assigned by default to the PCM Administrator role.

To create a new object type:

1. Choose **Physical** then **Configure**.
2. Choose **Types** then **Object Types**.
3. On the Configure Object Types page, click **Add** in the Object Types Table area.
4. On the Create or Edit Object Type page, specify the properties of the object type.
5. Click **Create**.

   A message appears confirming the object type was created successfully.
6. Click **OK**.

The new object type is now added to the list of object types on the Configure Object Types page and can be selected on the Create or Edit Physical Item page.

To edit an object type, choose **Edit Object Type** from the item's **Actions** menu.

16.1.3.3 Viewing Object Type Information

> **Note:**
>
> The PCM.Admin.Manager right is needed to perform this action. This right is assigned by default to the PCM Administrator role.

To view information about an existing object type:

1. Choose **Physical** then **Configure**.
2. Choose **Types** then **Object Types**.
3. On the Configure Object Types page, select the object type in the list of existing types and click the **Info** icon.
4. When finished, click **OK** to return to the Configure Object Types page.

16.1.3.4 Deleting an Object Type

> **Note:**
>
> The PCM.Admin.Manager right is needed to perform this action. This right is assigned by default to the PCM Administrator role.

To delete an existing object type:

1. Choose **Physical** then **Configure**.
2. Choose **Types** then **Object Types**.
3. On the Configure Object Types page, choose **Delete Object Type** from the **Actions** menu for the object. To delete multiple types, select the check box for the type then choose **Delete** from the Table menu.

   The object type is deleted, and a message to that effect is displayed.
4. Click **OK** to return to the Configure Object Types page.

16.1.3.5 Editing Object Type Relationships

> **Note:**
>
> The PCM.Admin.Manager right is needed to perform this action. This right is assigned by default to the PCM Administrator role.

To edit object type relationships:

1. Choose **Physical** then **Configure**.
2. Choose **Types** then **Object Types**.
3. On the Configure Object Types page, select the item to edit and choose **Edit Object Type Relationships** from the **Actions** menu.
4. On the Edit Object Type Relationships page, verify that the Assigned Object Types box contains all object types that can be contained within the current object type. If not, select the appropriate item in the Unassigned Object Types box and click **Add** to move it to the Assigned Object Types box.
5. Click **Submit Update** when finished.

   The object type relationships are updated, and the information page opens again with updated values for the **Object Type Hold** field.

16.1.4 Configuring Media Types

Media types are an extension to object types and provide a further specification about the type of content that can be contained in a storage location.

When creating a physical item, specify its media type. The available media types depend on the selected object type for the physical item. If you select a media type that is not allowed for the assigned storage location, an error message is displayed and you cannot check in the physical item.

The following topics are discussed regarding media types:

- Predefined Media Types
- Creating or Editing a Media Type
- Viewing Media Type Information
- Deleting a Media Type

16.1.4.1 Predefined Media Types

PCM comes with the following predefined media types.

Predefined Media Types	Object Type
Box	Box
Mixed Fax Paper Photo	Document
Folder	Folder
Mixed Microfiche Microfilm	Micro

Predefined Media Types	Object Type
Mixed CD Disc DVD BluRay	Optical
Mixed Audio Data Visual	Tape
Mixed Audio Box CD Data Disc Dvd BluRay Fax Folder Microfiche Microfilm Paper Photo Visual	All

16.1.4.2 Creating or Editing a Media Type

> **Note:**
>
> The PCM.Admin.Manager right is needed to perform this action. This right is assigned by default to the PCM Administrator role.

To create a new media type:

1. Choose **Physical** then **Configure**.
2. Choose **Types** then **Media Types**.
3. On the Configure Media Types page, click **Add** in the Media Types area.
4. On the Create or Edit Media Type page, specify the properties of the media type.
5. Click **Create**.

   A page opens confirming the media type was created successfully.
6. Click **OK**.

The new media type is now added to the list of media types on the Configure Media Types page and it can be selected on the Create or Edit Physical Item page.

To edit a media type, choose **Edit** from the media type's **Actions** menu. Modify the properties as needed and click **Submit Update**.

16.1.4.3 Viewing Media Type Information

> **Note:**
>
> The PCM.Admin.Manager right is needed to perform this action. This right is assigned by default to the PCM Administrator role.

To view information about an existing media type:

1. Choose **Physical** then **Configure**.
2. Choose **Types** then **Media Types**.
3. On the Configure Media Types page, click **Info** for the type to view.

   The Information page opens.
4. When finished, click **OK** to return to the Configure Media Types page.

16.1.4.4 Deleting a Media Type

> **Note:**
>
> The PCM.Admin.Manager right is needed to perform this action. This right is assigned by default to the PCM Administrator role.

To delete an existing media type:

1. Choose **Physical** then **Configure**.
2. Choose **Types** then **Media Types**.
3. On the Configure Media Types page, choose **Delete Media Type** from the **Actions** menu for the item to be deleted. To delete multiple items, select the check box for the item and choose **Delete** from the Table menu.

   The media type is deleted, and a message to that effect is displayed.
4. Click **OK** to return to the Configure Object Types page.

16.1.5 Configuring Default Metadata Values: Offsite and Reservations

> **Note:**
>
> The PCM.Admin.Manager right is needed to perform this action. This right is assigned by default to the PCM Administrator role.

If a user submits a reservation request for one or more items, a new content item is checked into the repository (in the Reservation security group). This content item automatically enters the Reservation Process workflow, if enabled, and the administrator receives a workflow review notification about the request.

After reviewing the reservation request, the administrator can further process the reservation request in accordance with the applicable procedures within the organization.

Default metadata values can be defined for the reservation items that are checked into the repository. Default metadata values can also be set for items that are allocated for offsite storage. The definition procedure is the same.

> **Note:**
>
> Offsite storage options only appear if Offsite Storage functionality is enabled. To check the status, choose **Physical** then **Configure** then **Settings**. Verify that the **Offsite** option is checked.

16.1.5.1 Setting Default Metadata Values for Reservations and Offsite Storage

To set the default metadata values for reservation items checked into the repository or defaults for offsite storage:

1. Choose **Physical** then **Configure**.
2. Choose **Metadata** then **Reservation Default Metadata**.
3. To configure offsite storage, choose **Physical** then **Configure** then **Offsite** then **Offsite Default Metadata**.
4. On the Default Metadata for Checked-in Reservation or Offsite Entries page, set the metadata values and click **Submit Update**.

The following defaults are set:

- The default content ID is `res` or `offsite`. This is a prefix added to the ID to create the full content ID of an item (for example, `res1430068` or `offsite3921`). This setting cannot be modified.
- The default content type is `REQUEST-PCM Request` or `OFFSITEREQUEST - Offsite Request`.

- The default title is `Reservation` for reservations and `Offsite Transfer Request` for offsite storage. This is a prefix added to the name to create the full title of an item (for example, `Reservation My Request`).
- The default security group is `Reservation` or `Offsite`.

> **Note:**
>
> You can change the content type and security group, but if you do, you need to modify your reservation process and workflow to match the new settings.

16.2 Configuring Storage Space

The following issues should be considered when planning storage space:

- At the root (top) level of the storage space hierarchy (Storage), only the two highest level location types can be added (Warehouse or Room) by default. If more location types are needed, modify the following configuration variable in the `physicalcontentmanager_environment.cfg` file:

  ```
  NumberOfStorageTypeRootsToShow=x
  ```

  where *x* is the number of location type levels needed at the highest storage level. For example, if users should be able to add storage locations of location types Warehouse, Room, or Row, change the value from 2 (default) to 3. Restart the Content Server for the change to take effect.
- There is no limit to the number of top-level storage locations that can be created (for example, one for each warehouse).
- At each level in the storage space hierarchy other than top level, only storage locations of a lower location type level can be added. For example, at the Row location type level, storage locations of the types Bay, Shelf, and Position can be added.
- Physical items not assigned to any other storage location are automatically assigned to the Other storage location, which is always the last of the top-level storage locations of the storage hierarchy.
- Storage locations can be deleted from the hierarchy only if no items are stored in them. The Other storage location cannot be deleted, even if it is empty.
- All storage locations include a percentage that shows how much of the available storage space in the location (and all its children) is currently occupied. For example, 25% means one quarter of the maximum allowed number of stored items is currently assigned to the storage location (and all its children). The percentage of a storage location is updated daily (see next note).
- By default, the available storage space for the entire hierarchy is recalculated daily at midnight. Therefore the storage availability information may not be up to date as the day progresses because it still reflects the situation from the night before. If you are an administrator with the `PCM.Admin.Manager` right, you can force a recalculation of all available storage space by running the Process Storage Space Counts batch service.
- A storage location can be blocked, which prevents any content from being stored in the storage location or any of its child storage locations, even if it was marked to allow storage of content. Only empty storage locations can be blocked. For example, this can be used to create a dummy storage location in a situation where a bay cannot be used

because there is a support pillar in front of it but matching bay numbering is necessary to retain across multiple rows.

- The `ShowContentForStorageBrowse` configuration variable can be used to hide or reveal content when browsing a storage location. Hiding content can speed response time during browsing. If set to TRUE, content is displayed. If set to FALSE, it is hidden.
- To speed response time during retrieval and browsing, set up storage so no one level has more than 100 items stored there. For example, set up a series of bays and each bay would contain 100 shelves with a maximum of 100 items on the shelf. This will speed up the browsing of objects in storage. It is also recommended that items be stored only at the shelf and position levels, not at the warehouse, room, row, or bay level. This will also speed retrieval and browsing times.

This section discusses the following topics:

16.2.1 Browsing the PCM Storage Space

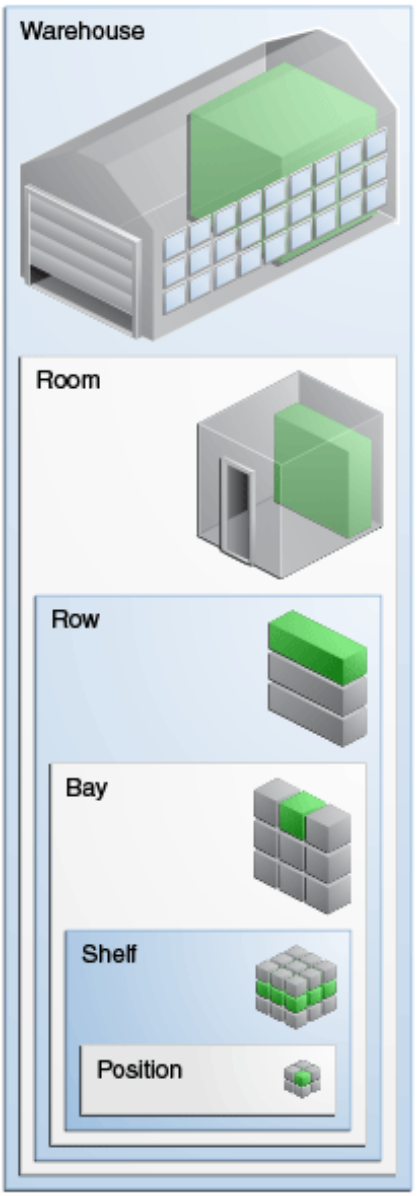
PCM uses a defined space environment to keep track of the storage and retention of physical items. When working with a physical item, assign the item to a storage location, so PCM knows where it is stored and can track it.

This section describes browsing the defined storage environment in PCM. It covers the following topics:

16.2.1.1 Storage Space Hierarchy

Storage space in PCM is set up hierarchically. Storage locations contain other, smaller storage locations that contain still smaller storage locations, and so on. The storage space hierarchy (from large to small) is provided by default.

Figure 16-1 Default Storage Space Hierarchy

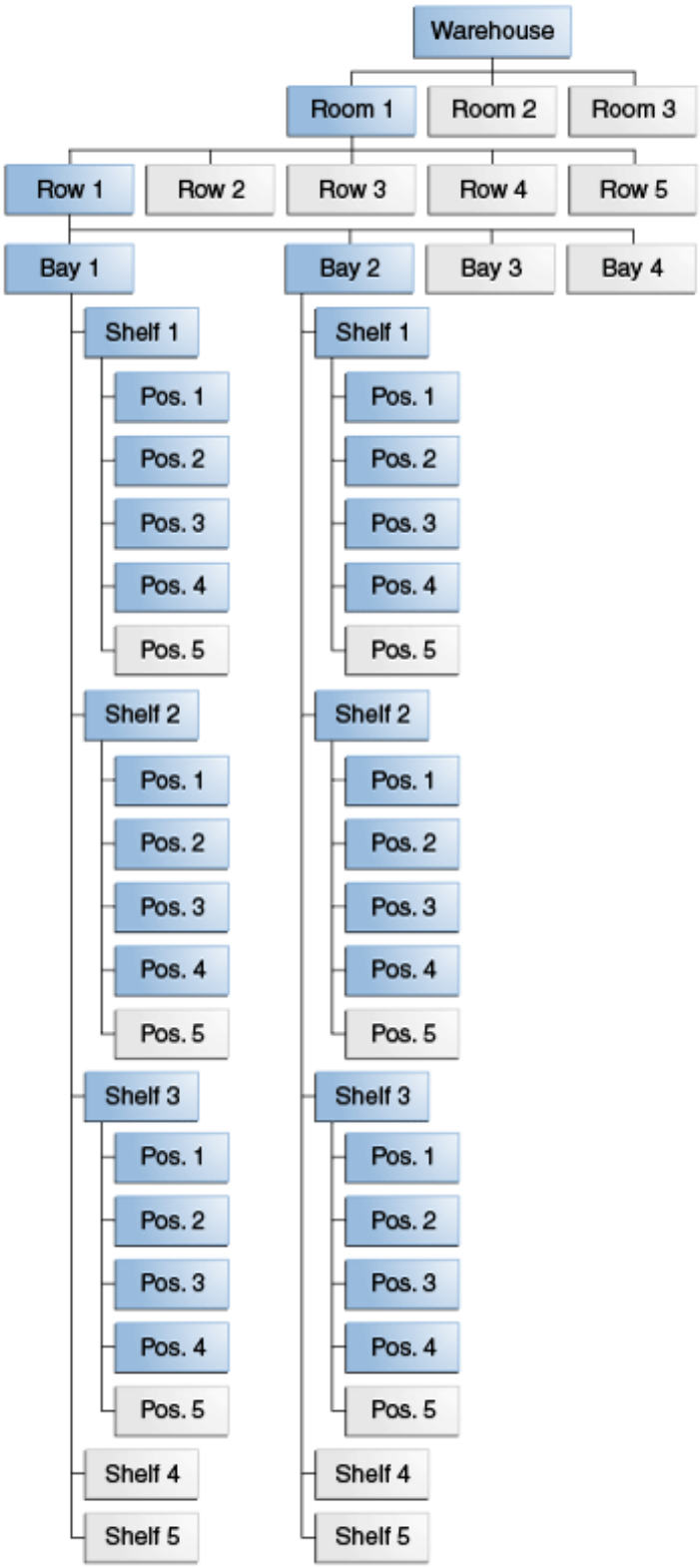


As shown in Figure 16-1, a warehouse consists of one or more rooms, a room consists of one or more rows, and so on. The further down in the hierarchy, the more specific (and smaller) the storage locations become.

The storage space environment you are working with may have different hierarchical levels, depending on how the physical content management feature has been set up for your organization.

Storage space can be depicted as in Figure 16-2, which is similar to a genealogy chart. The Warehouse at the top level contains rooms, which in turn contain rows. A row can contain a bay and a bay can contain shelves. Within each shelf distinct positions are noted for items.

Figure 16-2 Example Storage Space Environment



PCM keeps track of the use of space in the defined storage environment, and provides information about the available storage space on the Storage Information page of a storage location. Items cannot be stored in a location without sufficient space.

Storage locations can be added regardless of the parent location. For example, you can define a row or bay position in a warehouse.

> **Note:**
>
> By default, the available storage space is recalculated daily at midnight. Therefore the storage availability information may not be entirely up to date as the day progresses because it still reflects the situation from the night before.

16.2.1.2 Storage Location Properties

> **Note:**
>
> The type of allowed content storage applies to a particular level only. For example, in the default hierarchy, shelves have several positions, each of which can hold content items, but no content items can be directly assigned to the shelf level (only to the positions on a shelf). Therefore the location type `Shelf` cannot store content, whereas the type `Position` can.

Each storage location in the storage space environment has several properties:

- Location type: Each storage location is assigned a location type, which helps specify where it is located in the storage space hierarchy. The available location types are defined by your administrator.

  The following predefined location types (in hierarchical order) are provided:

  - Warehouse
  - Room
  - Row
  - Bay
  - Shelf
  - Position

  Storage of content applies to a particular level, not to lower levels. For example, shelves have a number of positions, each of which can hold content items, but no content items can be directly assigned to the shelf level (only to the positions on a shelf).

  These predefined location types are hierarchical: a warehouse consists of one or more rooms, a room consists of one or more rows, a row consists of one or more bays, and so on.

- Object type: The object type of a storage location in the storage space environment specifies what type of items the storage location can hold.

  The following predefined object types are provided:

  - All. An All object type cannot be assigned to a physical item.
  - Box
  - Document
  - Folder
  - Micro
  - Optical
  - Tape

  Administrator can also set up a different list of object types to meet the needs of an organization. When creating a new physical item, select its object type on the Create Physical Item page.

- Media Type: The media type of a storage location in the storage space environment provides a further specification of the type of items the storage location can hold.

  Several predefined media types are provided, but your administrator may also have set up a different list of media types to meet the needs of your organization.

  The available media types depend on the selected object type of the current storage location. The table below explains which predefined media types can be selected for each predefined object type.

Object type	Supports these media types
Box	Box
Document	Mixed Fax Paper Photo
Folder	Folder
Micro	Mixed Microfiche Microfilm
Optical	Mixed CD Disc DVD BluRay
Tape	Mixed Audio Data Visual

Object type	Supports these media types
All	Mixed Audio Box CD Data Disc Dvd BluRay Fax Folder Microfiche Microfilm Paper Photo Visual

16.2.1.3 Storage Status

If a storage location in the storage space can hold content items, its status determines whether content can be stored in the unit, and if not, why not. The status of a storage location is shown in the status column on the location page and can be any of the following:

- **Available**: Content can be stored in the storage location, and space is available. This is the default. If no status is provided, this one is assumed.
- **Reserved**: No content can be stored in the storage location or any of its child storage locations because it has been reserved. There may be space available in the storage location, but it has been set aside for future storage of physical items (for example, to ensure grouped storage of batches of items as they come in to be stored). If the logged-in user is the one who reserved the space, it will show as available to that person.
- **Occupied**: The storage location has reached its maximum storage capacity, and no further content can be added to it.

A user may have blocked a storage location. This prevents storage of content in a storage location even if space is available. If that is the case, the status column on the location page is empty.

16.2.2 Managing Storage Spaces

The following tasks are involved in managing storage spaces:

- Creating a Storage Location
- Batch Creating Storage Locations
- Editing a Storage Location
- Viewing Information about a Storage Location
- Deleting a Storage Location
- Blocking a Storage Location
- Reserving or Canceling a Reservation for a Storage Location

- Viewing All Items in a Storage Location
- Printing Labels for Storage Locations

16.2.2.1 Creating a Storage Location

> **Note:**
>
> The PCM.Storage.Create right is needed to perform this action. This right is assigned by default to the PCM Administrator role.

To create a new storage location in the storage space hierarchy:

1. Choose **Physical** then **Storage**.
2. To create a location at the topmost level of the hierarchy, choose **Create** then **Define Storage Location** from the page **Actions** menu. You can also choose **Create Storage Location** from the **Actions** menu for a storage location in the list to add a new child storage location at that level.
3. On the Create or Edit Storage page, specify the storage location properties:
   - **Storage Name**: Name for this storage area. Maximum characters allowed: 30.
   - **Description**: A brief description of the location. Maximum characters allowed: 30.
   - **Location Type**: The type of storage location. Select a type from the list. The available types depend on where the storage area is created in the storage hierarchy.
   - **Allow Storage of Content**: If selected, the storage location can hold content items. The default is the configured default setting for the selected location type, but it can be overridden if required.This does not have to be enabled if any of the location's child locations will hold content.

     For example, you may have a storage location of type `Shelf` with several positions, each of which can hold content items. If you do not want any items to be directly assigned at the shelf level but only to the positions on a shelf (stored at a position, not on a shelf), then you set the shelf storage location to not allow storage of content, and the position storage location to allow storage.

     If selected, all fields (except Requestor) below it become available.
   - **Status**: Available only for locations that can hold items. The status of the location (for example, `Available`).
   - **Requestor**: Available only for locations that can storage content and if the storage status is set to Reserved. Specifies the user who reserved the storage location.
   - **Location Holds**: Available for locations that can hold items. The type of physical items stored in the storage location. If an object type is not specified, the storage location can then hold any type of content. If an object type is selected and someone attempts to store an inappropriate object type, an error message is displayed and the physical item is not checked in.
   - **Maximum Items Allowed**: Available only for locations that can hold items. Specifies the maximum number of items the location can hold, used to track

space availability. If not specified, 1 (one) is assumed, which means only a single item can be assigned to the storage location.

- **Barcode**: Available only for locations that can hold items. The barcode for the item. If not specified, a random 19 digit number is assigned.
- **Addressing Information**: Address, city, state, zip code and other information for offsite storage location.
- **Offsite Ship To Code**: Only available when Offsite Storage is enabled. The Ship To code for offsite storage.

4. Click **Create** when done.

   The newly created storage location is now included in the storage space hierarchy at its assigned level.

16.2.2.2 Batch Creating Storage Locations

> **Note:**
>
> The PCM.Admin.Manager right is needed to perform this action. This right is assigned by default to the PCM Administrator role.

Batch creation is useful in situations where the storage hierarchy (or part of it) consists of a well-defined tree structure with consistent naming and numbering of its constituent objects. This procedure defines this storage location structure in one operation, without having to define each object separately.

You do not add the defined objects to the storage hierarchy directly from this page. Rather, specify the naming and numbering rules to be used to create the storage locations. After clicking **OK**, a file called `StorageImport.hda` is generated, which can be imported into the existing storage hierarchy.

To add several storage locations to the storage space hierarchy in a single batch:

1. Choose **Physical** then **Configure** then **Batch Storage Creation**.
2. On the Create Batch Storage Import File page, click **Browse**.
3. In the Select Storage Location dialog, navigate to the level in the storage hierarchy where the new storage location structure should be added and click **OK**.
4. Specify the rules and parameters to be used to create the batch of storage locations:
   - **Location Type**: Choose a location from the list of location types.
   - **Name Prefix**: A prefix for the storage name. This prefix is included in the name and the description of the storage location. If not specified, the name and description will contain only numbers (for example, `003`).
   - **Start Number**: The starting number for the number sequence that is included in the name and description of the storage location. If not specified, 1 (one) is assumed.
   - **Number of Items**: How many instances of the storage location to include in the storage space. The default number of digits used in the numeric sequences is 3, which will result in names such as `Warehouse_`*`NNN`* (for example, `Warehouse_003`).

The `AutoStorageNumberWidth` variable in the `storagecreationutility_environment.cfg` file can be modified to change this. Restart the Content Server after changing the value.

- **Allow Content**: If selected, items can be stored directly in the storage location. This applies to this storage location, not to any child locations. It is not necessary to enable this if any of child locations will hold content.

  For example, a Shelf storage location may have several positions, each of which can hold content items. To allow assigning of items only to the positions and not the shelf, do not select this option and set the position location to allow storage.

- **Number of Content Items Allowed**: Available if **Allow Content** is selected. Specify the maximum number of items the storage location can hold. Used to track space in the storage location. If not specified, 1 (one) is assumed (only one item can be assigned to the storage location.)

- **Object Type**: Available if **Allow Content** is checked. This designates the type of physical content items the storage location can hold from all defined object types.

  If not specified, the storage location can hold any type of physical content. If an object type is selected and someone attempts to store an inappropriate object type, an error message is displayed and the physical item is not checked in.

5. Click **Create** when finished to create the storage locations in accordance with the defined specifications, or click **Reset** to return the page to its initial values.

   A file called `StorageImport.hda` is generated, and a dialog opens that enables you to save this file to your hard drive.

   The newly created storage locations are now included in the storage space hierarchy at their assigned level.

   The following information should be considered when considering batch creation of storage locations:

   - When defining a storage space, you must obey the existing location type hierarchy. Start with the highest-level storage location and work your way down the hierarchy. You cannot add a parent location below a child location (for example, a shelf above a row). If you attempt to do this, error messages appear when you import the `StorageImport.hda` storage definition file.
   - The name and description of each generated storage location is built from the name prefix (if specified) and a sequential number such as `Warehouse_001`, `R003`, or `WH_NY-012`.
   - The default number of digits used in the numeric sequences is 3. To change the number of digits, modify the `AutoStorageNumberWidth` value in the `storagecreationutility_environment.cfg` file. Restart the Content Server after changing the value.

6. Click **OK**.

   The Exploring page opens again.

16.2.2.3 Editing a Storage Location

> **Note:**
>
> The PCM.Storage.Edit right is needed to perform this action. This right is assigned by default to the PCM Administrator role.

To edit the properties of an existing storage location:

1. Choose **Physical** then **Storage**.
2. Choose **Edit** then **Edit Storage Location** from the **Actions** menu of the item to edit.
3. On the Create or Edit Storage page, modify the storage location properties as required and click **Submit Update** when finished.

   A message appears stating the storage location was updated successfully, along with a list of the current storage location properties.

16.2.2.4 Viewing Information about a Storage Location

> **Note:**
>
> The PCM.Storage.Read right is needed to perform this action. This right is assigned by default to the PCM Administrator and the PCM Requestor role.

To view information about a storage location:

1. Choose **Physical** then **Storage**.
2. Click the **Info** icon for the storage location, or choose **Information** then **Storage Information** from the location's **Actions** menu.
3. Click **OK** when done.

   The Exploring page opens again.

This page shows the current properties of the selected storage location, including the total available spaces (calculated from all child storage locations) and the spaces currently used. There are also locator links at the top of the page, which show where the storage location is located in the storage space hierarchy.

By default, the available storage space is recalculated daily at midnight. Therefore, the storage availability information may not be up to date as the day progresses because it reflects the situation from the night before. If you are an administrator with the `PCM.Admin.Manager` right, you can force a recalculation of the available storage space by running the **Process Storage Space Counts** batch service.

16.2.2.5 Deleting a Storage Location

> **Note:**
>
> The PCM.Storage.Delete right is needed to perform this action. This right is assigned by default to the PCM Administrator role.

A storage location must be empty before it can be deleted. A location is considered empty if it does not contain any items. If a storage location has all empty child storage locations, the entire branch can be deleted. If you attempt to delete a non-empty storage location, an error message is displayed.

To delete a storage location:

> **Note:**
>
> You cannot delete the predefined Other storage location, even if it is empty.

1. Choose **Physical** then **Storage.**
2. Navigate to the storage location to delete, and choose **Delete** then **Delete Storage Location** from the item's **Actions** menu.

   To delete multiple storage locations from the exploring pages select their check boxes and choose **Delete** in the Table menu.

   If the storage location is empty, it is immediately deleted from the storage space hierarchy (without any further warnings), and the Exploring page is refreshed. If the storage location is not empty, an error message is displayed and it will not be deleted.

16.2.2.6 Blocking a Storage Location

> **Note:**
>
> The PCM.Storage.Block right is needed to perform this action. This right is assigned by default to the PCM Administrator role.

After blocking, no items can be stored in the location and all its child locations, even if space is available.

Only empty storage locations can be blocked. When a location is blocked, its Allow Storage of Content setting is set to No.

An example of use is to create a dummy storage location a storage bay cannot be used (because of physical limitations) but it is necessary to retain sequential numbering across multiple rows.

To block a storage location:

1. Choose **Physical** then **Storage.**
2. Navigate to the storage space level to block and choose **Edit** then **Block Storage** from the level's **Actions** menu.

   The initial Exploring page opens again and content can no longer be assigned to the storage location. If the status column previously showed **Available**, it is now empty. Also, the Storage Information page of the storage location has the **Allow Storage of Content** field set to **No**.

To cancel the blocked status of a storage location and allow storage of content again, edit the storage location and set its **Allow Storage of Content** setting to **Yes**. After unblocking a storage location, its status column on the Exploring pages shows **Available** again. It was empty while the storage location was blocked.

16.2.2.7 Reserving or Canceling a Reservation for a Storage Location

> **Note:**
>
> The PCM.Storage.Reserve right is needed to perform this action. This right is assigned by default to the PCM Administrator and PCM Requestor role.

If a storage location is reserved, all its child locations are also reserved. Only an administrator or the person who reserved a storage location can add items to it.

To reserve a storage location for future use:

1. Choose **Physical** then **Storage.**
2. Navigate to the storage space level that includes the storage location to reserve.
3. Choose **Edit** then **Reserve Storage** on the location's **Actions** menu.
4. Select the requestor reserving the space from the list of users.
5. The initial Exploring page opens again and the storage location now shows Reserved in its status column, with the name of the user who made the reservation in parentheses next to the status.

To cancel the reserved status of a storage location, navigate to a reserved location and choose **Edit** then **Cancel Request** on the **Actions** menu.

16.2.2.8 Viewing All Items in a Storage Location

> **Note:**
>
> The PCM.Storage.View right is needed to perform this action. This right is assigned by default to the PCM Administrator and PCM Requestor role.

To view all items currently contained in a storage location:

1. Choose **Physical** then **Storage.**

2. Navigate to the storage space level that includes the storage location with items to view. Choose **Change View** from the Table menu to view a graphical depiction of the storage hierarchy.
3. Click the storage name of a location to view items at that location.

16.2.2.9 Printing Labels for Storage Locations

> **Note:**
>
> The PCM.Admin.PrintLabel right is needed to perform this action. This right is assigned by default to the PCM Administrator role.

The label file contains the barcodes and other information for the current storage location and all its child storage locations if any exist. Only storage locations that can hold content items are included. Any intermediate storage levels are skipped if they cannot hold content.

By default, the label for a storage location contains a barcode uniquely representing the location, the location's name, its description, and its location type. The format of the label file depends on the Report Label Format setting on the Configure Physical Settings page.

If the generated label file is in PDF format, Adobe Acrobat Version 6.0 or later is needed to view it.

To create a label for a storage location:

1. Choose **Browse Content** then **Storage** or choose **Physical** then **Storage**.
2. Navigate to the storage space level.
3. Depending on the current storage location, choose **Create Reports** from the **Actions** menu for the location. Select one of the report types listed there.

You can also create a label for a storage location from the page menu on the Storage Information page. Choose **Create Report** then the report type. This menu contains an option to print a label only if the storage location can hold content.

16.2.3 Example: Creating a Single Storage Location

This example demonstrates how to create a storage location called `Warehouse_003`, of location type `Warehouse` at the top level of the storage hierarchy.

1. Choose **Browse Content** then **Browse Storage**.

   You can also access the top-level storage Exploring page from the Configure Physical Settings page.
2. Choose **Create Storage Item** on the menu bar at the top of the page.
3. On the Create or Edit Storage page, enter **Warehouse_003** as the storage name and description.
4. Click **Warehouse** as the location type.
5. Click **Create**.

The newly created storage location is now included in the storage space hierarchy at the top level.

16.2.4 Example: Creating a Batch of Storage Locations

This example demonstrates how to create the definition file for a storage space structure then import this file to create the defined storage space within Physical Content Management's storage environment. The storage space structure consists of one warehouse at the top level of the storage environment, with several subordinate storage locations. Each of the lowest-level locations (Position) may hold five items, which can be of any object type.

Creating the Batch Storage Definition File

To create the batch storage definition file:

1. Choose **Physical** then **Configure** then **Batch Storage Creation**.
2. On the Create Batch Storage Import File page, click **Browse** to select the highest point of the hierarchy. If not selected, the `Storage` level is defaulted.
3. In the Select Storage Location dialog, select a location and click **OK**. Provide these creation rules for Location Type, Name Prefix, Start Number, Number of items, Allow Content, Number Allowed, and Object Type:
   - Room, Room_, 1, 2, unchecked, empty, all
   - Warehouse, Warehouse_, 1, 1, unchecked, empty, all
   - Row, Row_, 1, 2, unchecked, empty, all
   - Bay, Bay_1, 1, 2, unchecked, empty, all
   - Shelf, Shelf_, 1, 2, unchecked, empty, all
   - Position, Position_, 1, 3, checked, 5, all

   If the values provided exceed the limit set for storage (default is 1000) an error message is displayed.
4. Click **Create**.

   A file download dialog opens.
5. Click **Save** to store the generated `StorageImport.hda` file on the local hard drive.

Importing the Batch Storage Definition File

To import the batch storage definition file into PCM:

1. Choose **Records** then **Import/Export** then **Archives**.
2. Unselect all items (including those under **Show External Sources**) except for **Include Storage**.
3. Click **Browse** next to **Archive File** to select the `StorageImport.hda` file saved earlier.
4. After selecting the file, click **Import**.

   The import adds the defined storage space to the existing storage hierarchy at the selected location.

16.3 Offsite Storage

Customers can integrate storage with Iron Mountain SafeKeeper PLUS and other offsite storage facilities.

> **Note:**
>
> Iron Mountain configurations will vary from customer to customer. Be sure to test the integration in a development instance before using for production data.

The Offsite Storage link is an automated interface process for daily inventory and activity management between the Records system and offsite storage. This interface provides the following features:

- The automated creation of requests, both reference and permanent, for boxes and files from offsite storage.
- The automated creation of pickup requests for new and re-filed boxes and files for storage and return to the offsite location.
- Transfer of transmittal and individual list data for new boxes and files, and transmittal and list maintenance for existing boxes and files.
- The creation of a nightly log file listing inventory transaction history for a given day. This serves as a confirmation and data synchronization between the two systems.

To use this functionality, first map default values for different types of storage file formats to districts where the content is stored. Types of file formats include legal storage, insurance, loans, medical, and other storage types. Default districts are provided and default values for the fields used for storage.

After setting up the mapping, specify the storage parameters on the check-in page for physical content. After the content is checked in, a criteria workflow can be started to handle the approval of items pending transfer. This workflow must be created and enabled before the Offsite functionality can work. See Setting Up Workflows for details. While not required, it is recommended that this workflow be used.

Iron Mountain is currently the primary offsite provider. After the appropriate configurations are in place, the files are first stored on the computer before being sent to and from Iron Mountain using File Transfer Protocol (FTP). After the files are compiled, they are uploaded to the `/toplus` directory in the software directory structure.

A confirmation file is sent from Iron Mountain and stored in the `/fromplus` directory in the Iron Mountain directory structure. A nightly history download log is also stored in the `/fromplus` directory after each night's district job is processed. Verify beforehand that the chosen FTP location has these directories already created.

Pickup lists are automatically created for items that must be transferred. Manual pickup lists can also be created as needed.

This section discusses the following topics:

- Setting Up Default Customer Information

- Mapping New Districts
- Creating Manual Pickup Requests
- Browsing Uploaded Files
- Browsing Processed Files
- Transferring Files to Offsite Storage

16.3.1 Setting Up Default Customer Information

First set up default customer information about the account to be used by the offsite provider. These defaults identify your company to the provider and are used to monitor and process offsite requests.

To configure defaults for offsite storage:

1. Choose **Physical** then **Settings**.
2. On the Configure Physical Content Management page, select **Enable Offsite Storage Functionality** then click **Submit Update**.
3. Refresh the browser window. Choose **Physical** then **Offsite Storage** then **General Setup**.
4. On the Offsite Storage General Setup page, fill in the necessary fields:
   - **Customer ID**: The customer ID used with this offsite storage facility.
   - **Default District**: The district to use. Select from a predefined list. If the district has not previously been defined, the definition must be mapped beforehand.
   - **FTP Address**: Enter the address associated with the FTP site.
   - **FTP User**: Enter the user associated with the FTP site.
   - **FTP Password**: Enter the password associated with the FTP site.
   - **Transfer** check boxes: Choose options associated with the transfer:
     - **Automatically transfer new items**: Enable automatic transfer of new items.
     - **Automatically return checked-in items**: Enable automatic returns of items that have been checked in.
     - **Enable workflow**: Start a workflow for this transfer action. The workflow must be created before this step. See Setting Up Workflows for details about creating the workflow.
     - **Use general requestor for Offsite Requests**: Choose a user from the list to use as the requestor. There is a limit of five characters for this value.
   - **Box Identifier**: Choose what identifier to associate with the box. Options include **Name** or **Title**.

   > **Note:**
   >
   > In addition to the existing options, you can also use the SFTP protocol to transfer files.

5. When done click **Submit Update**.

A message appears indicating the offsite storage data has been configured.

16.3.2 Mapping New Districts

Several default districts are provided with PCM to use for offsite storage. Reconfigure any of these districts as necessary for your particular offsite solution.

The district mapping uses a wizard that steps through each stage of the process. When one stage is finished, the wizard opens the next page in the process.

The values used to populate the option lists for each field are based on data provided by Iron Mountain. For details about the field values, consult Iron Mountain documentation.

To map district data:

1. Choose **Physical** then **Offsite Storage** then **Map District Metadata**.
2. On the Choose District Mapping page, select a district to configure from the list by scrolling through the list and highlighting a selection. Click **Configure** to select the district.
3. The next page in the wizard appears. The process for mapping information is the same on each page. Scroll through the values provided for the different fields and highlight a selection.

   Click **Save** to proceed to the next page in the process. Click **Exit the Wizard** to exit the process without saving selections. Click **Reset** to clear the selections on the current page. To move forward or back in the process and skip pages, select a different page from the page menu.

   Eight pages are available for configuration:

   a. Map box metadata
   b. Map standard file metadata
   c. Map account file metadata
   d. Map insurance (1) metadata
   e. Map insurance (2) metadata
   f. Map law metadata
   g. Map loan file metadata
   h. Map medical file metadata
4. When finished configuring districts, click **Save**.

   A message appears indicating a successful exit from the wizard.

16.3.3 Creating Manual Pickup Requests

This function can be used to create requests to the offsite storage provider for pick up of materials.

To set up pickup requests:

1. Choose **Physical** then **Offsite Storage** then **Create Manual Pickup Request**.
2. On the Create Manual Pickup page, select a district ID from the list of IDs.

3. Enter a pickup location or select a location by clicking **Browse** to look at stored locations.
4. Enter the remainder of the information on the page.
5. To discard entries, click **Reset**. When done, click **Submit Update**.

16.3.4 Browsing Uploaded Files

You can browse all of the uploaded files and view the status of the files. If a file has failed to upload, the upload request can be resent from this page.

To view files:

1. Choose **Physical** then **Offsite Storage** then **Uploaded Files List**.
2. To work with a file, select the box next to the file name. To delete a file, choose **Delete** from the Table menu or the item's **Actions** menu. To resend a file for processing, choose **Resend**.

16.3.5 Browsing Processed Files

You can browse all of the processed files and view the status of the files. If a file has errors, you can then use this page to correct the errors.

To view files:

1. Choose **Physical** then **Offsite Storage** then **Processed History Files List**.
2. To delete a file, check the box next to the file name then choose **Delete** from the Table menu or the item's **Actions** menu.

16.3.6 Transferring Files to Offsite Storage

Transferring files for offsite storage occurs in two stages: files must first be generated then transferred.

1. To generate files for files for transferring, choose **Physical** then **Offsite Storage** then **Generate Offsite Transfer Files**.
2. To upload, download, or process the files, choose **Physical** then **Offsite Storage** then **Upload, Download, Process Offsite Files**. The files will automatically transfer with other scheduled batch processes during the nightly services that are processed.

16.4 Managing Physical Items

As opposed to internal electronic content managed by content management products, no copy of external, physical content is stored in the repository. Only its metadata (including storage information and retention schedule, if any) is stored when the information is checked in to the system.

When a user checks in an external, physical content item, the user must provide its basic metadata information and specify where the item is stored by selecting a location in the defined storage space hierarchy. If the user has the appropriate privileges, a retention schedule can also be assigned to the item, which determines its life cycle.

Physical items can be created within other physical items. This may be useful in situations where a `container` physical item is needed (for example, of object type `Box` add `content` physical items within it (for example, of object type `Folder`).

This section discusses the tasks involved in managing physical items. Some tasks are allowed for administrators and for end users while others are restricted only to people with administrative privileges. The following user tasks are discussed in *Using Oracle WebCenter Content*:

- Creating a physical item
- Creating a physical item within another item
- Editing a physical item
- Moving a physical item
- Adding physical items to a content basket
- Marking physical items as reviewed
- Viewing reservations for physical items

The following tasks can be performed by administrators and are discussed in the following subsections:

- Deleting a Physical Item
- Freezing and Unfreezing a Physical Item
- Printing a Label for a Physical Item
- Importing Physical Content Manually
- Processing Physical Content

16.4.1 Deleting a Physical Item

> **Note:**
>
> The PCM.Physical.Delete right is required to perform this task. This right is assigned by default to the PCM Administrator role.

A physical item cannot be deleted if it has other physical items contained within it. When deleting a physical item, its metadata, storage, and retention information are removed from the repository. Therefore, the item can no longer be tracked and managed.

To delete a physical item:

1. Search for the physical item to delete.
2. On the search results page, choose the **Delete External Item** option in the item's **Actions** menu.

   You can also choose the **Delete External Item** option on the Physical Item Information page.

   The physical item is deleted immediately, without any further prompts. If no errors occur, a message is displayed stating the physical item was deleted successfully.

16.4.2 Freezing and Unfreezing a Physical Item

> **Note:**
>
> The Record.Freeze/Unfreeze right is required to perform this task. This right is assigned by default to the Records Administrator role. This right is not assigned by default to any PCM roles.

Freezing a physical item inhibits disposition processing for that item. For example, it will not be flagged for destruction, even if the action is due, until the item is unfrozen (when its frozen status is revoked). This may be necessary to comply with legal or audit requirements (for example, because of litigation).

More than one freeze can be applied to an item. View the freeze details for the item to see a list of all freezes currently applied to the item.

If a physical item containing other physical items is frozen, all of those items are also frozen. After a physical item is frozen, its metadata cannot be edited.

To freeze a physical item:

1. Search for the physical item to freeze.
2. On the search results page, choose **Edit** then **Freeze** in the item's **Actions** menu.

   You can also choose **Edit** then **Freeze** on the Physical Item Information page.

   To freeze all items on the search results page, choose the **Freeze Results** option in the page menu.
3. In the Freeze Name list, select the freeze to be applied to the item. The list contains all defined freezes. A reason can be given for the freeze or leave the text box empty.
4. Click **OK** to confirm the freeze. Click **Cancel** to abort the entire action.

   If confirmed, the information page of the affected item displays *Is Frozen: Yes* and a **Details** link, which links to a detailed page for the item.

After an item is frozen, the freeze reason cannot be edited. If the freeze is no longer correct, unfreeze the item and freeze it with a new reason.

To unfreeze a physical item (cancel its frozen status):

1. Search for the physical item to unfreeze.
2. On the search results page, choose **Edit** then **Unfreeze** in the item's **Actions** menu.

   You can also choose **Edit**, then **Unfreeze** on the Physical Item Information page.
3. In the Unfreeze dialog, select the freeze to be canceled for the item. The list contains all freezes currently applied to the item (at the item level). If needed, provide a reason for the unfreeze action or leave the text box empty.
4. Click **OK** to confirm. Click **Cancel** to abort the entire action.

   If confirmed, the Retention Schedule Information area of the Content Information page displays `Is Frozen: No` and no **Details** link is displayed.

> **Note:**
>
> Multiple freeze may be applied to an item. Therefore, after an item is unfrozen, the **Actions** menu for the item may continue to include an **Unfreeze** option if other freezes are still applied to the item.

16.4.3 Printing a Label for a Physical Item

> **Note:**
>
> The PCM.Admin.PrintLabel right is required to perform this task. This right is assigned by default to the PCM Administrator role.

By default, the label contains a barcode for the item, and its name, title, security group, and account (if applicable). To print a label:

1. Search for the physical item for which to print a label.
2. On the search results page, click **Create Report** then the type of label.

You can also choose the Print Label option on the Physical Item Information page.

16.4.4 Importing Physical Content Manually

If an import file already exists for physical content, that data can be imported into the system for tracking by PCM. This section describes the format for the file needed for correct importing.

The import file to be used must be an `.hda` file with three result sets: LocalDataProperties, ImportExportManifest, and ExternalItemsExtItems.

16.4.4.1 LocalDataProperties

This result set is used for the local data used by the Import service when importing the data. Set `aIncludeERM_Physical=1` for physical data to be imported.

```
@Properties LocalData
aIncludeERM_Physical=1
blFieldTypes= dCreateDate date,dLastModifiedDate date
blDateFormat='{ts' ''yyyy-MM-dd HH:mm:ss{.SSS}[Z]'''}'!tAmerica/Chicago
@end
```

If importing dates, the data must be in the format `{ts 'yyyy-mm-dd hh:mm:ss.mmm'}` if using the blDateFormat property set as shown in the Local Data result set. That format can be modified but imported dates must then be in the same format.

16.4.4.2 ImportExportManifest

This result set provides the import function with the necessary data to import physical items. This result set can be copied into an `.hda` file as is.

```
@ResultSet ImportExportManifest
28
Name
Order
Caption
ResultSetName
ExportScript
ExportConditions
ExportClass
ExportAction
ExportParameters
ExportActionCopy
ImportScript
ImportConditions
ImportClass
ImportAction
ImportParameters
ImportPassName
UpdateClass
UpdateAction
UpdateParameters
UpdatePassName
UpdateForced
DeleteClass
DeleteAction
DeleteParameters
DeletePassName
Group
dSource
idcComponentName
aIncludeERM_Physical
300
csaIncludeExternal
ExternalItemsExtItems
<$hasCustomRights("ecm.pcm.physical.read")$>

Service
EXPORT_EXTERNAL_ITEMS
dSource,Physical

<$hasCustomRights("ecm.pcm.physical.create")$>

Service
CREATE_EXTERNAL_ITEM


Service
EDIT_EXTERNAL_ITEM







content
Physical

@end
```

16.4.4.3 ExternalItemsExtItems

This result set contains the physical data being imported.

```
@Result Set ExternalItemsExtItems
11
dID 3 19
dDocName 6 100
dDocTitle 6 200
dDocAuthor 6 30
dDocType 6 30
dSecurityGroup 6 30
dPermLocation_Barcode 3 19
dActualLocation_Barcode 3 19
dExtObjectType 6 30
dMediaType 6 32
dSource 6 8
@end
```

> **Note:**
>
> Set only one location value for each current and permanent location. The following list shows multiple options for setting these values.

The following fields are required:

- **dID**: The document identifier. This field can be left blank, but the field has to be in the definition. The system assigns a value if this is left blank.
- **dDocName**: The document name.
- **dDocTitle**: The document title.
- **dDocAuthor**: The assigned author/creator.
- **dDocType**: The assigned document type.
- **dSecurityGroup**: The assigned security group.
- **dExtObjectType**: The object type for the item being imported (for example, a box or a document). The object type must exist in the system prior to importing.
- **dSource**: The source identifier. This must be set to `Physical`.
- **dPermLocation_Barcode**: The permanent location value. Set this value if the location value is the barcode value of the storage or container item where the object is being assigned.
- **dActualLocation_Barcode**: The current location value. Set this value if the location value is the barcode value of the storage or container item where the object is being assigned.
- **dPermLocation**: The permanent location value. Set this value if the location value is the dObjectID value of the storage item where the object is being assigned.
- **dActualLocation**: The current location value. this value if the location value is the dObjectID value of the storage item where the object is being assigned.

- **dPermContainer**: The permanent container location value. Set this value if the location value is the dID of the contain item where the object is being assigned.
- **dActualContainer**: Set this value if the location value is the dID of the contain item where the object is being assigned.

The following fields are optional:

- **dMediaType**: Used to assign a media type to an item.
- **dBarcode**: Used to provide a specific barcode for an item. Leave this blank and the system assigns the dDocName as the barcode.

Include any custom fields or other fields required for import.

16.4.4.4 Sample File

The following sample file demonstrates all result sets in an `.hda` file.

```
<?hda version="10.1.3.5.1 (090717)" jcharset=UTF8 encoding=utf-8?>
@Properties LocalData
aIncludeERM_Physical=1
blFieldTypes=xRecordFilingDate date,xArchiveDate date,xRecordCutoffDate
date,xRecordExpirationDate date,xRecordObsoleteDate date,xNewRevisionDate
date,xPublicationDate date,xRecordActivationDate date,xRecordSupersededDate
date,xRecordCancelledDate date,xRecordDestroyDate date,xDateClosed
date,xRecordRescindedDate date,xNoLatestRevisionDate date,xDeleteApproveDate
date,xRecordReviewDate date,xSuperSupersededDate date,dCreateDate
date,dLastModifiedDate date
aIncludeChargeTransactions=0
dLastModifiedDate={ts '2009-06-01 17:00:00.000'}
aExportDate=6/01/09 5:00 PM
blDateFormat='{ts' ''yyyy-MM-dd HH:mm:ss{.SSS}[Z]'''}'!tAmerica/Chicago
@end
@ResultSet ImportExportManifest
28
Name
Order
Caption
ResultSetName
ExportScript
ExportConditions
ExportClass
ExportAction
ExportParameters
ExportActionCopy
ImportScript
ImportConditions
ImportClass
ImportAction
ImportParameters
ImportPassName
UpdateClass
UpdateAction
UpdateParameters
UpdatePassName
UpdateForced
DeleteClass
DeleteAction
DeleteParameters
DeletePassName
Group
```

```
dSource
idcComponentName 6 30
aIncludeERM_Physical
300
csaIncludeExternal
ExternalItemsExtItems
 <$hasCustomRights("ecm.pcm.physical.read")$>

Service
EXPORT_EXTERNAL_ITEMS
dSource,Physical

<$hasCustomRights("ecm.pcm.physical.create")$>

Service
CREATE_EXTERNAL_ITEM


Service
EDIT_EXTERNAL_ITEM




content
Physical

@end
@ResultSet ExternalItemsExtItems
11
dID 3 19
dDocName 6 100
dDocTitle 6 200
dDocAuthor 6 30
dDocType 6 30
dSecurityGroup 6 30
dPermLocation_Barcode 3 19
dActualLocation_Barcode 3 19
dExtObjectType 6 30
dMediaType 6 32
dCreateDate 5 20
dSource 6 8

B0000003050
ImportTestBox
sysadmin
ADACCT
Public
TSTIMPORT
TSTIMPORT
Box

{ts '2009-06-04 11:50:50.497'}
Physical

F0000003050
ImportTestFolder
sysadmin
```

```
ADACCT
Public
B0000003050
B0000003050
Folder

{ts '2009-06-04 11:50:50.497'}
Physical
@end
```

16.4.5 Processing Physical Content

This section explains how to process physical items used by PCM. It discusses the following topics:

- Retention Schedules for Physical Items
- Disposition Events for Physical Items
- Pending Options for Physical Items
- Audit Log Files for Processed Events

16.4.5.1 Retention Schedules for Physical Items

Physical items can be assigned retention schedules that define their life cycle. This links the physical item to a set of retention and disposition rules, which specify how long an item should be stored and when and how it should be disposed.

The same retention schedules and disposition rules may be used for physical items as for electronic items, but disposition rules can be defined specifically for physical items.

16.4.5.2 Disposition Events for Physical Items

A disposition event is any action needing to be performed on an item as part of its retention schedule (for example, after the retention period of the item has ended). Disposition events for physical items consist of three steps:

1. Approving the event.
2. Performing the action(s) associated with the event such as physical destruction of the affected item(s).
3. Marking the event as completed.

> **Note:**
>
> The Destroy disposition event requires two steps for physical items, but not for electronic items. This is because the software can destroy electronic items for you, but it cannot destroy physical items. Destruction of physical items requires human intervention.

Physical items can be assigned the same disposition actions as electronic items. See Defining and Processing Dispositions for details.

Due to the nature of physical items, some of the available disposition actions are less relevant than for electronic items:

- Disposition actions related to revisions because physical items cannot be revisioned:
  - Deleting old revisions
  - Checking in new revisions
  - Deleting previous revisions
  - Deleting revisions
  - Deleting all revision
- Disposition actions involving digital data:
  - Scrubbing data. This includes overwriting it multiple times to prevent recovery as part of the destruction process.

If any of these disposition actions are assigned to physical items and they are due for completion, nothing specific needs to be done and they can be marked completed immediately.

16.4.5.3 Pending Options for Physical Items

Any pending events for physical items are included on the My Approval List page. To access this page, choose **Records** then **Approvals**. Choose the type of approval to perform:

- Reviews
- Dispositions

To complete an action such as approval, review or a disposition, choose the appropriate completion action from an item's **Actions** menu. Some dispositions require approval before disposition processing.

> **Note:**
>
> If the event action does not move to the completion list, then all affected items are frozen and cannot be processed. If the event action does move but also remains in the approval list, some affected items are frozen. The frozen items will not be processed until they are unfrozen.

16.4.5.4 Audit Log Files for Processed Events

When a disposition event for physical items is completed, an audit log file is created automatically and, if possible, is checked into the repository using the default metadata for audit logs. These checked-in log files can be used for audit trail purposes or as a verification tool.

Use the Search Audit Trail page to search for disposition event that were processed for physical items by setting the Source field to 'Physical'.

The Admin.Audit right is required to search the audit trail.

> **Note:**
>
> All completed disposition actions are included in the audit trail.

16.5 Managing Reservations and Barcodes

Reservations in Physical Content Management are handled using a special criteria workflow called ReservationProcess, which is used for approval and notification purposes. This workflow must be configured and enabled. See Setting Up Workflows for details about setting up that workflow.

The reservation workflow is not used if the **Check in internal content item for reservation workflow** setting on the Configure Physical Content Management page is disabled. Users can still make reservations but email notifications are not received (not even by the system administrator). If this is done, a different procedure to process reservations should be in place.

Users with the predefined PCM Requestor role can make reservations for physical items. Users with the predefined `pcmadmin` role can also edit and process reservation request.

By default, if a user submits a reservation request for one or more items, a new content item is checked into the repository in the Reservation security group. If the workflow is enabled, this content item automatically enters the ReservationProcess workflow and the administrator receives a workflow review notification about the request.

Default metadata values can be set to be assigned to the reservation workflow item checked into the repository. See Configuring Default Metadata Values: Offsite and Reservations for details.

The person in the administrator role receives email notifications about pending reservations and the requesting user is not notified. Change this behavior by changing the ReservationGroup alias in the User Admin utility. For example, you could set up the workflow to also send email notifications to the user who made the reservation request.

Clicking the **Review workflow item** link in the notification email opens the Workflow Review for Request page, where the administrator can acknowledge the reservation request. As soon as the administrator clicks **Approve** on this page, the reservation request exits the workflow.

The administrator can then proceed and fulfill the reservation request in accordance with the applicable procedures within the organization.

By default, each user can place only one reservation request for the same item. If users make reservation requests on behalf of multiple people (for example, manager assistants), it may be useful to override this behavior. To do so, add the following variable to the `physicalcontentmanager_environment.cfg` configuration file:

```
AllowMultipleRequests=true
```

All completed reservation requests are automatically logged in the reservations history. A reservation request is considered completed if none of its request items are still pending (in process), on a waiting list, or checked out.

By default, completed reservation requests are stored in the history log until it is deleted. A log is kept in the audit history table until it is archived. Limit the maximum number of days a

completed request is included in the history by modifying settings on the Configure Physical Content Management page.

An administrator can view the current reservations history by searching for reservations with the Completed field set to `Yes`.

This section discusses the following topics:

- Understanding the Reservation Process
- Using Barcodes
- Managing Barcodes
- Specifying PCM Barcode Values for Users

16.5.1 Understanding the Reservation Process

The following is a typical fulfillment process of a reservation request:

1. A user creates a reservation request for one or more physical items.
2. As soon as the user submits the reservation request, the status of each requested item is automatically set to **In Process**. If it was already In Process or Checked Out, it is set to Waiting List.
3. A reservation workflow is initiated and the administrator receives an email notification to review the reservation request.
4. The administrator acknowledges the reservation request. If any items in the reservation request are not available or should be denied, the administrator can change their status accordingly.
5. All available requested items (not already checked out) are gathered from their storage location, in accordance with the organization's procedures. During this process, an appropriate transaction barcode is scanned to indicate it is checked out, the requestor's barcode is scanned, and the barcode for the item is scanned.
6. The status of each available requested item is changed to Checked Out automatically after the barcode file is uploaded to PCM and the data is synchronized.
7. When the item's status changes to Checked Out, its current location (as shown on the Physical Item Information page) is automatically set to the deliver-to location specified when the reservation request was created. If no deliver-to location was specified, the current location is set to `OTHER`. The current location comment on the Physical Item Information page is set to the location comment specified for the associated reservation request. If no comment was provided, it is set to the login name of the user who made the reservation.
8. The requesting user can be notified and the reservation fulfilled in accordance with the applicable procedures within the organization. This is not handled by PCM but by the organization.
9. The user keeps the items for a specific number of days. If a bar code system is in place, after the item is returned, the item's barcode is again scanned, the barcode for the location of the item's placement is scanned, and a transaction barcode is scanned to indicate the item is checked in and its location.
10. The status is changed to Returned and its current location set to its assigned storage location automatically after the barcode file is uploaded to PCM.

11. If a waiting list exists for the item, the status for the next requestor on the list should be changed from Waiting List to In Process, so the item can be processed for the user. This can be done manually on any of the reservation pages, but if a barcode scanner is used to scan the item for checkin, it can be done automatically, depending on how the system is configured.
12. The status of the item continues to be Returned until the reservation is deleted. This can be done manually or automatically (after a certain number of days).

Depending on the procedures in place at the site, a charge may be levied for reservations and processing. Chargebacks and billing are discussed in *Using Oracle WebCenter Content*.

16.5.1.1 Reservation Request Properties

Each reservation request has properties:

- **Request Status**: Specifies the current status for a reserved physical item, which can be any of the following:
  - **Waiting List**: The request item is currently already checked out to someone else. It becomes available to the next requestor upon its return (unless the system administrator chooses to override the waiting list order).
  - **In Process** (initial default): The reserved item is available and is being prepared for delivery. Only one request item for a reservation can have the In Process status.
  - **Not Found**: The request item could not be located in its designated location.
  - **Unavailable**: The request item cannot currently be processed for delivery.
  - **Denied**: The reservation request has been rejected by the administrator and cannot be fulfilled.
  - **Cancelled**: The reservation request was called off before it could be fulfilled.
  - **Checked Out**: The reserved item is currently in the possession of someone as part of a reservation request. If a physical item is checked out, its current location (as shown on the Physical Item Information page) is automatically set to the value of the Deliver To Location field for the associated reservation request. If no value was entered in this field, the current location is set to `OTHER`. Also, the current location comment as shown on the Physical Item Information page) is set to the location comment specified for the associated reservation request. If no comment was provided, it is set to the login name of the user who made the reservation.
  - **Overdue**: The reserved item is currently checked out to someone who has failed to return the item within the configured checkout time. As a result, the reservation request cannot currently be fulfilled.

    By default, an email notification is sent out to the user who has an overdue item. This email notification can be disabled.
  - **Returned**: The checked-out item was returned to the storage repository, so it is available for other users to reserve and check out.

  A reservation request is considered completed if none of its request items are still pending (in process), on a waiting list, or checked out (including overdue).

  The PCM.Reservation.Process right is required to change the status of a reservation request item. By default, this right is assigned to the predefined 'pcmadmin' role.
- **Transfer method**: specifies how the person who made the request (the requestor) will receive the reserved item. Users specify the transfer method when a reservation request is created. The following transfer methods are supported:

  - **Copy**: The physical content item is duplicated and the copy provided to the intended recipient. The copy can be physical (for example, a copied DVD) or electronic (for example, an ISO image of a CD).
  - **Fax**: The physical content item is faxed to its intended recipient.
  - **Mail**: The original physical content item is mailed to its intended recipient.
  - **Pickup**: The intended recipient picks up the physical content item in person.
  - **Email**: The content item is emailed to its intended recipient.
- **Priority**: specifies the urgency with which it needs to be fulfilled. User specify the priority when they create a reservation request. The following priorities are supported:
  - **No Priority**: Delivery of the requested item does not have any particular priority (there is no rush). The item can be delivered in accordance with the applicable fulfillment procedures.
  - **ASAP Rush**: The requested item should be delivered to its intended recipient as soon as possible after the reservation was made.
  - **This Morning**: The requested item should be delivered to its intended recipient the same morning the reservation was made.
  - **Today**: The requested item should be delivered to its intended recipient the same day the reservation was made.
  - **This Week**: The requested item should be delivered to its intended recipient the same week the reservation was made.

  The default priority is set on the Configure Physical Content Management page.

16.5.1.2 Request Item Actions

If you are an administrator, you can perform actions on a request item to change its status as part of the reservation fulfillment process. These actions are accessible through the Actions menu for a request item on the Reservation Search Results page or the Items for Request page. You can also perform the actions on multiple items simultaneously using the Actions menu on the Items for Request page.

Not all actions may be available for a particular request item, depending on the item's current status. For example, if the item is currently checked out, it can only be deleted or returned.

The following actions are supported:

- **Delete**: Deletes an item from a reservation request. If deleted, the request for that item is not included in the reservation log. The item is no longer in the item list for the reservation request. This option is available only if the system has been set up to allow users to delete items from a reservation request. In addition, requested items can be deleted only by a user with the PCM.Reservation.Delete right (assigned to the predefined PCM Administrator role by default).
- **Deny**: Rejects the reservation request for an item. The item will remain to be part of the reservation request, but it will not provided to the requestor.
- **Not Found**: Changes the status of an item because it could not be located in its designated location. The item will remain to be part of the reservation request, but it cannot currently be provided to the requestor.

- **Unavailable**: Changes the status of an item because it cannot currently be processed for delivery. The item will remain to be part of the reservation request, but it cannot currently be provided to the requestor.
- **Cancel**: Cancels the reservation request for an item before it is fulfilled. If a request item is cancelled, the request for that item is still included in the reservation log (the item is still on the item list for the reservation, with its status set to cancelled). Request items can be cancelled only users with the PCM.Reservation.Edit right (assigned to the predefined pcmadmin role by default). Only request item with the In Process status can be cancelled.
- **Check Out**: Changes the status of an item because it was handed off to its intended recipient, who can now keep the item for the configured checkout period. After checking out a request item, its current location (as shown on the Physical Item Information page) is automatically set to the value of the Deliver To Location field for the associated reservation request. If no value was entered in this field, the current location is set to `OTHER`. Also, the current location comment shown on the Physical Item Information pageis set to the location comment specified for the associated reservation request. If no comment was provided, it is set to the login name of the user who made the reservation.
- **Returned**: Changes the status of a checked-out item because it was returned handed off to its intended recipient, who can now keep the item for an agreed period.

16.5.2 Using Barcodes

Barcode files are generated by barcode devices that scan storage information contained in barcodes located on physical content items or storage containers. A barcode is a machine-readable symbol used to store bits of data. In the context of physical content management, they can be used for purposes of identification, inventory, tracking, and reservation fulfillment.

Figure 16-3 Example of Barcode

Barcodes can be printed on labels attached to physical content items or storage containers holding such items (for example, a box). This helps track their location and status. User labels can also be created to help process reservation requests by users.

> **Note:**
>
> View barcode reports using HTML but print reports using PDF in order to ensure proper formatting.

The following technical information applies to barcodes in PCM:

- PCM uses the Code 3 of 9 barcode standard (also called Code 39). This is a widely used standard for alphanumeric barcodes that can store upper-case characters, decimal

numbers, and some punctuation characters (dash, period, dollar sign, slash, percent sign, and plus symbol).

- All lower-case letters are automatically converted to upper case. For example, if a user login is `jsmith` then its barcode value is `JSMITH`.
- Any accented letters and double-byte characters (such as Japanese and Korean) are encoded in their hexadecimal values. For example, if a user login is `kmüller`, then its barcode value is `KMC39CLLER` (Ü =hex C39C). Therefore the barcode length increases as multiple hexadecimal characters are used to represent each accented letter or double-byte character.
- Barcode values for users default to their login names. This behavior can be changed for a user by setting a specific, unique barcode value for the user in the User Admin utility.

After scanning barcode information using a barcode reader, load the information into Physical Content Management. This can save time and money, and is especially useful to process large numbers of items (for example, during the initial PCM implementation).

There are two ways to load barcode information into PCM:

- Directly using the PCM Barcode Utility software.
- Manually by processing generated barcode file.

16.5.2.1 Barcode Files

Barcode files are generated by barcode scanners that read storage information from barcode labels and write this information to a file. Use the optional PCM Barcode Utility to directly load barcode information into the system or the barcode file can be processed manually.

Barcode files are plain-text files that are viewable using any text editor, such as the following example.

```
H 20050721130204 00 0000000000
20050721130145 00 2000
20050721130151 00 +W1R1R1B1S1P3
20050721130152 00 B3
```

> **Note:**
>
> Barcode files are created by barcode scanners and processed by PCM, and there is normally no reason to view or modify barcode files.

When a barcode file is processed (automatically or manually), one of three actions is performed (specified for each item in the barcode file):

- **Check in**: this action assigns an item to the location specified in the barcode file for the item. It is only the current location that is set, not the permanent location. Both the location and the item must already exist in PCM. If neither exists, an error is reported.

  The location must already exist in the defined storage space hierarchy in PCM. If an item to be checked in does not yet exist in PCM, it is created and assigned to

the specified location. If the item already exists, its current location is updated to match the value in the barcode file.

- **Check out**: this action checks an item out to the user specified in the barcode file for the item (typically obtained by scanning a user label). The status for the item is set to Checked Out and its checkout user to the specified user (both values are shown on the Physical Item Information page). The item's current location is automatically set to the value of the Deliver To Location field for the associated reservation request (if there is one). If no value was entered in that field or if no reservation request exists, the current location is set to `OTHER`, and the Location Comment field will show the name of the checkout user.
- **Set Home and Actual**: this action assigns an item to the current and permanent locations specified in the barcode file for that item, allowing it to be moved to a different location. Both the locations and the item must already exist in PCM. If any of them do not exist, an error is reported.

  The locations and items must already exist in the defined storage space hierarchy in PCM. The item's current and permanent locations are updated to match the values in the barcode file.

16.5.2.2 The Barcode Utility Software

The Barcode Utility software is a Windows application providing an interface to the Videx LaserLite barcode scanner used with PCM. With this functionality, information can be read into the barcode scanner and uploaded into PCM. The barcode information can also be read and written to a file for manual processing at a later time. In addition, the Barcode Utility enables the reprogramming of the barcode scanner, should that be necessary.

The Barcode Utility software for Videx is provided but not automatically installed with the PCM software. To use, install the software after enabling PCM. The installer for the Barcode Utility is included on the PCM software distribution media.

Microsoft .NET Framework Version 1.1 Redistributable Package is needed to run the Barcode Utility. If not already on the computer, it can be downloaded from the Microsoft website at www.microsoft.com

The Barcode Utility can be installed on any computer that has a web connection to the server.

> **Note:**
>
> When upgrading the Barcode Utility from an earlier version, you *must* de-install the existing instance before installing the new release. If this is not done, an error message is reported during the installation and you will not be able to proceed.

To install the Barcode Utility:

1. Locate the executable installer file, named `BarcodeUtility.exe` on the PCM distribution media. This is typically stored in the `ucm\Distribution\urm\`*`language`* directory (different files are included for the different languages that are supported).
2. Double-click the `setup.exe` file to continue the installation.
3. Follow the instructions to install the software.

4. From **Start**, choose **Programs**, then **Oracle**, then **Barcode Utility**, then **Barcode Utility**. You can also double-click the utility icon on the Windows desktop.

   An interface is also provided to a Wedge Reader type of scanner that plugs in directly to the computer. If that type of scanner is enabled, data is automatically uploaded to a location where the cursor rests after three scans have taken place.

16.5.3 Managing Barcodes

This section discusses the following common barcode tasks:

- Programming the Barcode Scanner
- Uploading Barcode Data Directly
- Saving Barcode Data to a File
- Uploading Previously Saved Barcode Data
- Processing a Barcode File

16.5.3.1 Programming the Barcode Scanner

The Videx Wand scanner may be pre-programmed for use at installation. Use the following procedure, if needed, to program the barcode scanner:

1. Start the Barcode Utility application.
2. On the Main Barcode Utility page, choose **Options** then **Program Videx Wand**.
3. On the Program Videx Barcode Wand page, choose the type of scanner to be programmed from the **Communication Device** list.
4. Choose the communication port where the device is connected.
5. Click **Program**.

   A message appears indicating that the application is communicating with the scanner. The dialog closes when the programming finishes.
6. Click **Done** on the Main Barcode Utility page.
7. Push the **Scan** button on the scanner.

16.5.3.2 Uploading Barcode Data Directly

After gathering data with the scanner, the data can be directly uploaded to the server running the PCM software. The data can also be saved to a file and uploaded later.

To upload the scanned barcode data directly to PCM:

1. Connect the scanner to the computer where the Barcode Utility is installed, either by placing the scanner in its base station or by using the connection cable.
2. Start the Barcode Utility application. The Main Barcode Utility page opens.
3. Select the scanner type.
4. Select the communication port where the barcode scanner is installed. Normally this is COM1, a commonly used serial port.
5. Verify that **Download To File Only** and **Allow File Selection** are both deselected.
6. Click **Process**.

A prompt appears to begin the upload process.

7. Select **Yes** to continue.
8. Select the host name of the instance where data files will be uploaded. The software must be installed on this computer.

   To configure the list of available hosts:

   a. Click **Advanced**.
   b. On the Configure Host List page, enter the name of the instance where the repository is stored and the CGI URL for the instance.
   c. Click **Update** to add multiple names.
   d. Click **Done** when finished.
9. Enter the user name and password for a person who is allowed to upload data. To upload data, the user must have the predefined PCM Administrator role. Click **OK** after selecting the user name.

   The data is now transferred from the scanner to the PCM system. After all data has been transferred, a message is displayed, indicating the operation is complete.
10. Click **OK** to continue.

> **Note:**
>
> If you select **No** when asked to confirm the upload, the data is erased from the barcode scanner and nothing is uploaded. The data is still available in a file called `DATA.TXT` (located in the installation directory of the Barcode Utility), but this file is overwritten the next time data is uploaded or saved to a file.

16.5.3.3 Saving Barcode Data to a File

To save the scanned barcode data to a file:

1. Connect the scanner to the computer where the Barcode Utility is installed, either by placing the scanner in its base station or by using the connection cable.
2. Start the Barcode Utility application.
3. On the Main Barcode Utility page, select the scanner type.
4. Select the communication port where the barcode scanner is installed. Normally this is COM1, a commonly used serial port.
5. Select **Download To File Only**.
6. Click **Process**.

   The data is stored in a file called `DATA.TXT`, which is located in the installation directory of the Barcode Utility.

> **Note:**
>
> Data is always stored in a file named `DATA.TXT`. If not renamed, the file is overwritten the next time data is downloaded and stored as a file.

16.5.3.4 Uploading Previously Saved Barcode Data

If barcode data was saved to a file for later processing, use the Barcode Utility application to move the data to the PCM software for use.

To upload a previously saved barcode data file:

1. Start the Barcode Utility application.
2. On the Main Barcode Utility page, select **Allow File Selection** and click **Process**.

   A file selection dialog is displayed, showing the contents of the Barcode Utility installation directory (which is the default location of saved barcode data files).
3. Select the file to be uploaded, or navigate to the directory where the data files were stored and select a file from that location. Click **Open**.
4. On the Barcode Upload page, select the host name of the instance where the data file will be uploaded. The software must be installed on this computer.

   To configure the list of available hosts:

   a. Click **Advanced**.

   b. On the Configure Host List page, enter the name of the instance where the repository is stored and the CGI URL for the instance.

   c. Click **Update** to add multiple names.

   d. Click **Done** when finished.
5. Enter the user name and password for a person who is allowed to upload data. To upload data, the user must have the predefined PCM Administrator role.
6. Click **Submit**.

   The barcode data file is processed and uploaded to the selected instance.
7. After the file upload has completed, a message is displayed. Click **OK**.

   The Barcode Upload Results page opens, allowing a review of the results of the upload.
8. Click **Done** when finished.

16.5.3.5 Processing a Barcode File

> **Note:**
>
> The PCM.Barcode.Process right is required to perform this action. This right is assigned by default to the PCM Administrator role.

To process a barcode file containing information obtained using a barcode scanner:

1. Choose **Physical** then **Process Barcode File**.
2. On the Barcode Processing page, click **Browse** to select a barcode file to be processed.
3. In the file selection dialog, navigate to the barcode file to be processed, select it, and close the file selection dialog.
4. Click **Process File**.
5. The barcode file is processed, and the Barcode File Processed page opens. If any errors occurred, these are reported in the Message column. Click the **Info** icon to see more specific information about the error message.
6. When finished viewing the results of the barcode processing, click **OK** to return to the Barcode Processing page.

16.5.4 Specifying PCM Barcode Values for Users

Barcodes are used with PCM, which is only available when that software is enabled.

By default, the barcode value for a user consists of a user's login name in all upper-case letters, for example `JSMITH` or `MJONES`. If you do not want to use the login name of a user as the barcode value, use the User Admin utility to specify a different value for the user.

This is especially useful for login names containing characters other than the basic letters (a-z, A-Z) or numbers (0-9) (for example, accented letters such as `kmüller`). By default, the barcode values generated for such users include hexadecimal representations of the accented letters (for example, `KMC39CLLER`). To avoid this behavior set specific barcode values for these users (for example, `KMULLER`), which are then used rather than the (converted) user login names.

You can run the `Update Users with no Barcode` batch service to automatically set the barcode values for all users who currently do not have a barcode value. This is useful for users who are already in the system before PCM was enabled. The barcode values are set in accordance with the rules above.

To manually set a specific barcode value for a user:

1. Log in as an administrator.
2. Click **Administration** then click **Admin Applets**.
3. Click the **User Admin** icon.

   The User Admin utility is started.
4. On the **Users** tab, select the user whose barcode value should be set and click **Edit**.
5. In the Edit User dialog in the **Barcode** field, specify a unique value for the user. This value is used in the barcode label for the user rather than the user's login name (in all upper-case letters) as specified in the Name field.

   The specified value must be unique for each user in the system. An error message is displayed if a value is used that is not unique.

   Do not use any accented letters in the barcode value (an error message is displayed if you try). Also, any lower-case letters are automatically converted to upper case after clicking **OK**.
6. Click **OK** when finished.
7. Close the User Admin utility.

17

Processing Reservations and Chargebacks

This chapter discusses the processing of charges and invoicing as well as the reservation process for Physical Content Management. Not all tasks discussed here can be performed by all users. Access to functionality depends on assigned rights and roles.
Chargebacks are fees charged to people or businesses for the use of storage facilities or actions performed on physical items in the storage facilities. They can also be used to provide an explanation for storage actions. Reservations are used to manage physical items which can be checked out to users, reserved for later use, or requested.

This chapter covers the following topics:

17.1 Managing Chargebacks

Invoices can be generated for the storage, use, reservation, and destruction of the managed content. The invoices can then be sent to internal or external customers in accordance with applicable business procedures.

The administrator sets up *charge types* (billable events), *payment types* (methods of payment), and *customers* (users or organizations who will be billed). After being set, each billable action (creation, reservation, storage, destruction) can be charged to a particular customer by creating invoices containing one or more transactions on physical items occurring for these customers. Automatic transactions are those in which the charges are calculated at transaction time.

A **charge type** is a defined transaction triggered by certain criteria. For example, the creation of a physical item of object type Box and media type Box may cost $5 per occurrence, while reservation of an item with priority ASAP Rush may cost $20.

Whenever someone performs an action meeting the criteria of a charge type, a billable transaction is recorded for the associated user or organization (customer). The system uses the most specific charge type. If charge type A has two criteria and charge type B has the same two criteria plus another one, charge type B is recorded for a transaction meeting all three criteria of charge type B even though it also meets the two criteria of charge type A.

An amount of money is associated with each charge type that can be per item or for a specific period.For example, you could charge a fee every time a physical item is created (or reserved or destroyed), or charge a monthly fee to store a physical item.

A **payment type** specifies how internal or external customers pay for services. Pre-defined payment types include credit card or check. Custom payment types can also be created.

Customers are internal or external users or organizations who are charged for the services rendered on physical items. They will receive the invoices generated by Physical Content Management (in accordance with the applicable business procedures) and make the payments for the chargebacks.

After the charge types, payment types, and customers are defined, they can be used to create **invoices** to submit to the customers for each billable event. Invoices can be run on an as-needed basis or they can be scheduled automatically in accordance with defined criteria.

This section discusses the following topics:

- Understanding the Chargeback Process
- Configuring Chargeback Processing
- Managing Chargeback Tasks

17.1.1 Understanding the Chargeback Process

A site's specific reservation process may differ from the one described here, depending on the procedures in place.

The typical fulfillment process of a chargeback is as follows:

1. A user performs a billable action (for example, creates, reserves, or stores a physical item in storage).

   If automatic transactions are enable, when the user performs one of these actions on the physical item, those items are matched against all defined charge types. Each action on each item is matched against current transactions. If there is no match to a transaction, the action will not be recorded for chargeback.
2. The transaction is recorded in the system. The administrator should make sure there are transactions in place to cover as many variations as possible regarding actions on physical items. In this way chargeback can be made more automatic and require less individual attention for each request made for a physical item.
3. The administrator generates an invoice, either automatically through using scheduled invoices or manually by generating individual invoices.
4. The invoice is sent to the customer according to business procedures. The Physical Content Management functionality does not email invoices or otherwise deliver them.
5. The bill is paid or otherwise considered paid according to company procedures.
6. After the bill is paid, the administrator marks the invoice as paid within the Physical Content Management feature.

17.1.2 Configuring Chargeback Processing

Administrators set up charge types, payment types, and customers.

> **Note:**
>
> The PCM.Admin.Manager right is required to perform this action. This right is assigned by default to the PCM Administrator role. In addition, the chargeback feature has its own set of rights that define what users can do in this area.

The default Physical Content Management functionality comes with the following predefined charge actions:

- **Creation**: A user is billed if a physical item is created.
- **Destruction**: A user is billed if a physical item is destroyed.
- **Reservation**: A user is billed if a reservation request is made for a physical item.
- **Storage**: A user is billed if a physical item is stored.

The default Physical Content Management functionality comes with the following predefined payment types:

- Credit Card: To charge a customer paying with a credit card.
- Check: To charge a customer paying by check.

This section discusses the following topics:

17.1.2.1 Creating or Editing a Charge Type

> **Note:**
>
> The PCM.Admin.Manager right and the CBC.ChargeBacks.Create right are needed to perform this action. These rights are assigned by default to the PCM Administrator role.

The most specific charge type is always used. For example, if charge type A has two criteria and charge type B has the same two criteria plus another one, charge type B is recorded for a transaction meeting all three criteria of charge type B (even though it also meets the two criteria of charge type A).

To create a new charge type to be used for chargebacks:

1. Choose **Physical** then **Configure**. Choose **Charges** then **Type**.
2. On the Configure Charge Type page, click **Add**.

3. On the Create or Edit Charge Type page, specify the properties of the charge type.
   - Charge Type ID: Unique identifier for the charge type. Maximum: 30 characters. This field is view-only on the Edit Charge Type page.
   - Description: Description of the charge type. Maximum: 60 characters.
   - Actions: Type of action associated with the charge type. Options include Creation, Destruction, Reservation, or Storage.
   - Charge Amount: Amount charged for the transaction in dollars and cents and frequency of the charge (per item or per period).
   - Frequency: If Action is set to Storage, this is the frequency of the storage period.
   - Object Types: Object type that triggers the charge type. Click **Browse** to view and select an object type from a list.
   - Media Types: Media type that triggers the charge type. Click **Browse** to view and select a media type from a list.
   - Transfer Method and Priorities: When Action is set to Reservation, this is the transfer method of reservation that triggers the charge type.

   The new charge type is now added to the top of the list on the Configure Charge Type page.

> **Note:**
>
> The PCM.Admin.Manager right and the CBC.ChargeBacks.Edit rights are needed to perform this action. These rights are assigned by default to the PCM Administrator role.

To modify a page, select the item to edit in the list of items and choose **Edit Charge Type** from the item's **Actions** menu. Modify the properties as required and click **OK** when finished.

17.1.2.2 Viewing a Charge Type

> **Note:**
>
> The PCM.Admin.Manager right and the CBC.ChargeBacks.Read right are needed to perform this action. These rights are assigned by default to the PCM Administrator role.

To view the properties of a charge type:

1. Choose **Physical** then **Configure**. Choose **Charges** then **Type**.
2. In the list of charge types on the Configure Charge Type page, select the item and click the item's **Info** icon. The Payment Type Information page opens listing all properties of the charge type.

17.1.2.3 Deleting a Charge Type

> **Note:**
>
> The PCM.Admin.Manager right and the CBC.ChargeBacks.Delete right are needed to perform this action. These rights are assigned by default to the PCM Administrator role.

To delete a charge type:

1. Choose **Physical** then **Configure**. Choose **Charges** then **Type**.
2. In the list of charge types on the Configure Charge Type page, select the item to edit, and choose **Delete Charge Type** in the item's **Actions** menu or select an item's check box and choose **Delete** in the Table menu.

17.1.2.4 Creating or Editing a Payment Type

> **Note:**
>
> The PCM.Admin.Manager right and the CBC.ChargeBacks.Create right are needed to perform this action. These rights are assigned by default to the PCM Administrator role.

To create a new payment type to be used for chargebacks:

1. Choose **Physical** then **Configure**. Choose **Charges** then **Payment Methods**.
2. On the Configure Payment Methods page, click **Add**.
3. On the Create or Edit Payment Method page, specify the properties of the payment type, and click **OK**.

   The new payment type is now added to the bottom of the list on the Configure Payment Methods page.

> **Note:**
>
> The PCM.Admin.Manager right and the CBC.ChargeBacks.Edit right are needed to perform the following action. These rights are assigned by default to the PCM Administrator role.

To modify a payment type, select the item to edit in the list of items and choose **Edit Payment Type** from the item's **Actions** menu. Modify the properties as required and click **OK** when finished.

17.1.2.5 Viewing a Payment Type

> **Note:**
>
> The PCM.Admin.Manager right and the CBC.ChargeBacks.Read right are needed to perform the following action. These rights are assigned by default to the PCM Administrator role.

To view the properties of a payment type:

1. Choose **Physical** then **Configure**. Choose **Charges** then **Payment Methods**.
2. In the list of payment types on the Configure Payment Methods page, select the item and click the item's **Info** icon.

   The Payment Type Information page opens listing all properties of the payment type.

17.1.2.6 Deleting a Payment Type

> **Note:**
>
> The PCM.Admin.Manager right and the CBC.ChargeBacks.Delete right are needed to perform the following action. These rights are assigned by default to the PCM Administrator role.

To delete a payment type:

1. Choose **Physical** then **Configure**. Choose **Charges** then **Payment Methods**.
2. In the list of payment types on the Configure Payment Methods page, select the item to edit, and choose **Delete Payment Type** from the **Actions** menu.

17.1.2.7 Creating or Editing a Customer

> **Note:**
>
> The PCM.Admin.Manager right and the CBC.ChargeBacks.Create right are needed to perform the following action. These rights are assigned by default to the PCM Administrator role.

To create a new customer to be used for chargebacks:

1. Choose **Physical** then **Configure** from the Top menu. Choose **Charges** then **Customers**.
2. On the Configure Customers page, click **Add**.

3. On the Create or Edit Customer page, specify the properties of the customer:
   - Customer ID: Unique ID for the group being billed. Maximum characters: 30.
   - Name: Descriptive name for the customer. Maximum characters: 60.
   - Address and Contact Information: Address and contact information, including email or phone.
   - Is Active: Indicator of the active status of the customer. Default: no.

   The new customer is now added to the bottom of the list on the Configure Customers page.

> **Note:**
>
> The PCM.Admin.Manager right and the CBC.ChargeBacks.Edit right are needed to perform the following action. These rights are assigned by default to the PCM Administrator role.

To modify a customer, select the customer to edit in the list of customers and choose **Edit Customer** from the **Actions** menu on the customer list. Modify the properties as required and click **OK** when finished.

17.1.2.8 Viewing a Customer

> **Note:**
>
> The PCM.Admin.Manager right and the CBC.ChargeBacks.Read right are needed to perform the following action. These rights are assigned by default to the PCM Administrator role.

To view the properties of a customer:

1. Choose **Physical** then **Configure**. Choose **Charges** then **Customers**.
2. In the list of customers on the Configure Customers page, select the item and click the item's **Info** icon. The Customer Information page opens listing all properties of the customer.

17.1.2.9 Deleting a Customer

> **Note:**
>
> The PCM.Admin.Manager right and the CBC.ChargeBacks.Delete right are needed to perform the following action. These rights are assigned by default to the PCM Administrator role.

To delete a customer:

1. Choose **Physical** then **Configure**. Choose **Charges** then **Customers**.
2. In the Configure Customers page, in the list of customers, select the item to delete, and choose **Delete Customer** in the item's **Actions** menu. To delete multiple customers, select the check box for the customers and choose **Delete** from the Table menu.

17.1.2.10 Creating Automatic Transactions

Automatic transactions can be defined by selecting the transaction type and enabling it. To enable automatic transactions:

1. Choose **Physical** then **Configure**. Choose **Charges** then **Automatic Transactions**.
2. On the Configure Automatic Transactions page, select the transaction that should be made automatic by selecting the transaction's check box.
3. When finished, click **Submit Update**.

17.1.2.11 Creating or Editing a Manual Transaction

You can create a manual transaction in much the same way as creating automatic transactions. To add a manual transaction:

1. Choose **Physical** then **Configure**. Choose **Charges** then **Manual Transactions**.
2. On the Create Manual Transaction page, enter the necessary information for the transaction.
3. When finished, click **Create**.

17.1.2.12 Deleting a Manual Transaction

> **Note:**
>
> The PCM.AdminManager right, the CBC.ChargeBacks.Delete right, and the CBC.ChargeBacks.Admin right are required to perform this task. These rights are assigned by default to the PCM Administrator role.

To delete a transaction:

1. Choose **Physical** then **Configure**. Choose **Chargebacks**.
2. On the Charge Invoices page, select the link to **Transactions with No Invoice**.
3. In the list of transactions, select the **Delete** check box for the one to delete.

17.1.3 Managing Chargeback Tasks

This section discusses the processing of charging, invoicing, and billing. It contains the following topics:

- Creating or Scheduling an Invoice
- Adjusting an Invoice

- Deleting an Invoice
- Viewing Invoice Information
- Printing an Invoice
- Marking an Invoice As Paid

17.1.3.1 Creating or Scheduling an Invoice

> **Note:**
>
> The PCM.AdminManager right, the CBC.ChargeBacks.Create right, and the CBC.ChargeBacks.Admin right are required to perform this task. These rights are assigned by default to the PCM Administrator role.

To manually create a new invoice:

1. Choose **Physical** then **Invoices**. Choose **Chargebacks**.
2. On the Invoices page, click **Add**.
3. Select the content criteria used to screen for items to be included on the invoice (for example, records from a certain department).
4. Enter the necessary additional criteria to filter the transactions. Click **Generate Invoice** to create an invoice immediately or click **Schedule**. Click **Schedule** to open a scheduling page where schedule criteria can be entered.
5. Click **OK** when done.

17.1.3.2 Adjusting an Invoice

> **Note:**
>
> The PCM.AdminManager right, the CBC.ChargeBacks.Edit right, and the CBC.ChargeBacks.Admin right are required to perform this task. These rights are assigned by default to the PCM Administrator role.

To edit an invoice:

1. Choose **Physical** then **Invoices**.
2. On the Invoices page, choose **Edit** then **Adjust Invoice** in the **Actions** menu for an item. A page opens where information about the invoice can be adjusted.

17.1.3.3 Deleting an Invoice

> **Note:**
>
> The PCM.AdminManager right, the CBC.ChargeBacks.Delete right, and the CBC.ChargeBacks.Admin right are required to perform this task. These rights are assigned by default to the PCM Administrator role.

To delete an invoice:

1. Choose **Physical** then **Invoices**.
2. In the list of invoices on the Invoices page, select the check box next to the invoice then choose **Delete** from the Table menu.

17.1.3.4 Viewing Invoice Information

> **Note:**
>
> The PCM.AdminManager right, the CBC.ChargeBacks.Read right, and the CBC.ChargeBacks.Admin right are required to perform this task. These rights are assigned by default to the PCM Administrator role.

To view an invoice:

1. Choose **Physical** then **Invoices**.
2. On the Invoices page, click the **Info** icon for the invoice with information to view.

17.1.3.5 Printing an Invoice

> **Note:**
>
> The PCM.AdminManager right, the CBC.ChargeBacks.PrintInvoices right, and the CBC.ChargeBacks.Admin right are required to perform this task. These rights are assigned by default to the PCM Administrator role.

To print an invoice:

1. Choose **Physical** then **Invoices**.
2. On the Invoices page, choose **Reports** from the **Actions** menu for the invoice to print, and choose the type of report to produce.

17.1.3.6 Marking an Invoice As Paid

> **Note:**
>
> The PCM.AdminManager right, the CBC.ChargeBacks.Admin right, and the CBC.ChargeBacks.Edit right are required to perform this task. These rights are assigned by default to the PCM Administrator role.

To mark an invoice as paid:

1. Choose **Physical** then **Invoices**.
2. On the Invoices page, choose **Edit** then **Mark Paid** in the **Actions** menu for the invoice to mark as paid.

17.2 Processing Reservations

Reservations are used to manage physical content. A user can put a hold on items that are currently unavailable (for example, someone else has the item). If others also made a reservation request for an item, that reservation is put on a waiting list, which specifies the order in which people made a reservation for the item. A reservation request may comprise multiple items.

After a reservation request is made, an email notification is sent to the administrator, who processes the request and starts the reservation fulfillment process in accordance with the applicable procedures in the organization.

If you are a user with the standard reservation privileges, you cannot make any changes to an existing reservation. You can only do so if your administrator has granted you special privileges beyond the defaults for a PCM requestor.

Each user can normally place only one reservation request for the same item. However, the administrator may have set up the system so a user can make multiple requests. This may be useful in environments where there are users who make reservation requests on behalf of several people.

This section discusses the following topics:

- Reservation Request Properties
- Managing Reservations

17.2.1 Reservation Request Properties

Each reservation request has several properties, including the following:

- Request Status
- Transfer Method
- Priority

17.2.1.1 Request Status

The request status specifies the current status for a reserved physical item, which can be any of the following:

- **Waiting List**: The request item is currently already checked out to someone else. It becomes available to the next requestor upon its return (unless the administrator chooses to override the waiting list order).
- **In Process** (initial default): The reserved item is available and is being prepared for delivery. Only one request item for a reservation can have the In Process status.
- **Not Found**: The request item could not be located in its designated location.
- **Unavailable**: The request item cannot currently be processed for delivery.
- **Denied**: The reservation request has been rejected by the administrator and cannot be fulfilled.
- **Canceled**: The reservation request was called off before it could be fulfilled.
- **Checked Out**: The reserved item is currently in the possession of someone as part of a reservation request. If a physical item is checked out, its current location (as shown on the Physical Item Information page) is automatically set to the value of the Deliver To Location field for the associated reservation request. If no value was entered in this field, the current location is set to OTHER. Also, the current location comment on the Physical Item Information page) is set to the location comment specified for the associated reservation request. If no comment was provided, it is set to the login name of the user who made the reservation.
- **Overdue**: The reserved item is currently checked out to someone who has failed to return the item within the configured checkout time. As a result, the reservation request cannot currently be fulfilled.

  By default, an email notification is sent out to the user who has an overdue item. This email notification can be turned off.
- **Returned**: The checked-out item was returned to the storage repository, so it is available for other users to reserve and check out.

17.2.1.2 Transfer Method

The transfer method specifies how the person who made the request (the requestor) will receive the reserved item. Users specify the transfer method when a reservation request is created. The following transfer methods are supported:

- **Copy**: The physical content item will be duplicated and the copy will be provided to the intended recipient. The copy can be physical (for example, a copied DVD) or electronic (for example, an ISO image of a CD).
- **Fax**: The physical content item will be faxed to its intended recipient.
- **Mail**: The original physical content item will be mailed to its intended recipient.
- **Pickup**: The intended recipient will pick up the physical content item in person.
- **Email**: The content item will be emailed to its intended recipient.

17.2.1.3 Priority

The priority of a reservation request specifies the urgency with which it must be fulfilled. User specify the priority when they create a reservation request. The following priorities are supported:

- **No Priority**: Delivery of the requested item does not have any particular priority (there is no rush). The item can be delivered in accordance with the applicable fulfillment procedures.
- **ASAP Rush**: The requested item should be delivered to its intended recipient as soon as possible after the reservation was made.
- **This Morning**: The requested item should be delivered to its intended recipient the same morning the reservation was made.
- **Today**: The requested item should be delivered to its intended recipient the same day the reservation was made.
- **This Week**: The requested item should be delivered to its intended recipient the same week the reservation was made.

17.2.2 Managing Reservations

The following tasks are included when managing reservations:

- Creating a Reservation Request
- Editing a Reservation Request
- Deleting a Reservation Request
- Viewing Reservations for a Physical Item
- Changing the Status of a Request Item

17.2.2.1 Creating a Reservation Request

> **Note:**
>
> The PCM.Reservation.Create right is required to perform this task. This right is assigned by default to the predefined PCM Requestor and PCM Administrator roles.

Reservation requests can only be made for physical items. Error messages are displayed if an attempt is made to reserve electronic items.

By default, each user can place only one reservation request for the same item. If users make reservation requests on behalf of multiple people (for example, manager assistants), it may be useful to override this behavior. To do so, add the following variable to the `physicalcontentmanager_environment.cfg` configuration file:

```
AllowMultipleRequests=true
```

If a reservation request is created for a physical item containing other items, the other items are included in the reservation. The child items are not seen in the request, but when a checkout is done for the parent item, all child items are also checked out. A request can be

made for each of the child items, but they cannot be checked out until the parent item is returned.

As soon as a reservation request is submitted, the status of all request items is automatically changed to In Process, unless their status is already In Process or Checked Out. In that case, it is changed to Waiting List.

Users with the standard reservation privileges (those with the predefined 'pcmrequestor' role) cannot make any changes to an existing reservation by default. In order to edit reservation requests, they must be given the PCM.Reservation.Edit right.

To make a reservation request:

1. Search for the physical item(s) to reserve and add them to the content basket.
2. Choose **My Content Server** then **My Content Basket**.
3. On the Content Basket page, select the check box of each physical item to reserve and choose **Request** then **Request Selected Items** from the Table menu. To reserve all items in the content basket, choose **Request All Items**.

   A prompt is displayed asking if the selected items should be removed from the content basket after they are reserved.
4. Click **Yes** or **No**. Click **Cancel** to stop the reservation request.
5. On the Create or Edit Request page, specify the properties of the new reservation request:
   - Request Name: Name for the reservation. Note that this is not required to be unique. Each reservation request has a unique system-internal reference. The system tracks reservation requests using this internal reference, not the request name. Therefore, multiple reservations can have the same name. Maximum characters: 30.
   - Request Date: Date and time the request is made. Default is the current date and time.
   - Requestor: Person submitting the request. Default is currently logged-in user.
   - Security Group: Group to which the request is assigned. Security groups can be used to limit the requests to which users have access.
   - Transfer Method and Priority: Transfer method and priority to be used.
   - Required By Date: Date when the items are needed. Click the calendar icon to select a date. Providing a time is optional. If not specified, midnight (12:00) is used.
   - Deliver To Location and Location Comment: Location where the item should be delivered. If the location is in the storage hierarchy, click Browse to search for and select the location. If not in the hierarchy, use the Comment field to provide delivery details. If an item is checked out, its current location (as shown on the Physical Item Information page) is automatically set to the value of this field for the associated reservation request. If no value was entered, the current location is set to OTHER.
   - Comments: Additional comments as needed.
6. Click **Create** when finished.

The status of all request items is now automatically changed to In Process, unless their status is already In Process or Checked Out. In that case, it is changed to Waiting List. The items are reserved and the administrator is notified about the reservation

request. After the administrator processes the reservation request, it can be fulfilled in accordance with the procedures in the organization.

17.2.2.2 Editing a Reservation Request

> **Note:**
>
> The PCM.Reservation.Edit right is required to perform this task. This right is assigned by default to the predefined PCM Administrator role. A user can edit an owned reservation without this right depending on the settings when PCM was configured.

To modify the properties of a reservation request:

1. Choose **Physical** then **Reservations**.
2. On the Reservation Search Results page, locate the reservation request to edit and choose **Edit** then **Edit Request** from its **Actions** menu.
3. On the Create or Edit Request page, modify the properties of the reservation request and click **Submit Update** when finished.

17.2.2.3 Deleting a Reservation Request

> **Note:**
>
> The PCM.Reservation.Delete right is required to perform this task. This right is assigned by default to the predefined PCM Administrator role. A user can delete an owned reservation without this right depending on the setting when PCM is configured.

To delete a reservation request (and effectively cancel it):

1. Choose **Physical** then **Reservations**.
2. On the Reservation Search Results page, locate the reservation request to delete and choose **Delete Request** from its **Actions** menu.

   The reservation request is deleted immediately, without any further prompts. If there were no errors, a message is displayed stating the reservation request was deleted successfully.

17.2.2.4 Viewing Reservations for a Physical Item

> **Note:**
>
> The PCM.Reservation.Read right is required to perform this task. This right is assigned by default to the predefined PCM Requestor and PCM Administrator roles.

To view all outstanding reservation requests for a physical item:

1. Search for the physical item.
2. On the search results page, choose **Information** then **View Reservations** in the item's **Actions** menu.
3. The Reservation Search Results page opens listing all outstanding reservation request for the current physical item.

17.2.2.5 Changing the Status of a Request Item

> **Note:**
>
> The PCM.Reservation.Edit right is required to perform this task. This right is assigned by default to the predefined PCM Administrator role. Users can change the status of an owned reservation without this right depending on the settings when PCM was configured.

To change the status of a request item in a reservation request:

1. Search for the request item to change.
2. On the Reservation Search Results page locate the request item with statuses to change and choose **Information** then **Request Item Information** from its **Actions** menu.
3. On the Request Item Information page, choose **Edit** on the Page menu.
4. On the Edit Request Item page, select a new status and click **Submit Update** when finished.

18

Configuring Related Content (Links) for Records

This chapter provides information on configuring links to establish a relationship between content items in Oracle WebCenter Content: Records.
This chapter covers the following topics:

- Understanding Content Links
- Predefined Relationship Types
- Linking Methods
- Managing Related Content
- Link Examples

18.1 Understanding Content Links

Links establish a type of relationship between content items. Examples include a native file (created with software such as Word) that has several different renditions such as a PDF or thumbnail image, each of which is checked into the repository as a separate content item. These renditions can be linked to indicate a dependency on each other.

Relationships are based on one of four available Relationship Classes. Several Predefined Relationship Types are also provided but custom relationship types can be added to suit the need of the site environment.

> **Note:**
>
> You can create relationships between items only to which you have access. You cannot create relationships to items for which you do not have adequate access privileges such as assigned rights, classification, supplemental markings, and so on.

There are two basic methods of creating relationships between items:

- Creating a relationship from one item to another item: If a relationship is created from an item in the system to another item in the system, the search page can used during the process to access the item and link to it. For details see Linking to an Existing Item.
- Creating a relationship from an existing item to a new item: If a relationship from an item is added to a new item, use the content check-in page during the process to create the new item. For details see Linking to a New Item.

> **Note:**
>
> When items are deleted, all corresponding relationships are deleted, except in the case when a superseded content item is in the midst of disposition processing. A "dangling relationship" exists until the superseded content item completes its disposition processing. Then the relationships are deleted.

18.2 Predefined Relationship Types

The following predefined relationship types are available:

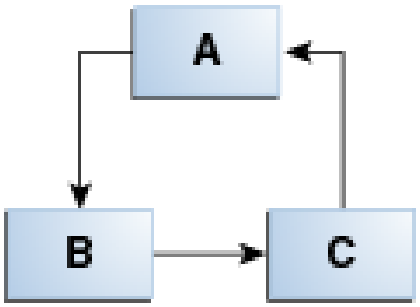
- Renditions, based on the Peer-to-Peer Class
- Supersedes, based on the Chained List Class
- Supporting Content, based on the Supporting Content Class
- Cross-Reference, based on the Cross-Reference Class

You can also define your own relationship types.

18.2.1 Renditions

The predefined Renditions type is based on the Peer-to-Peer Class. It is typically used to indicate peer relationships between items. Rendition in this sense means a link to a copy or some other version of an item. For example, an editable text item could be linked to a non-editable content item, or a physical printed rendition. This type of relationship can be created by anyone in the RecordsGroup security group to link an item source file to any other renditions.

Figure 18-1 Renditions Links



For example, all versions of a file may be a different graphic type: `.psd`, `.jpg`, and `.tif`. Figure 18-1shows A (`.psd`) is linked to B (`.jpg`), and B is linked to C (`.tif`). Item C is linked indirectly by association to A, but it is not actually linked directly to A. If the link between A and B is removed (unlinked), then C is no longer linked by association to A.

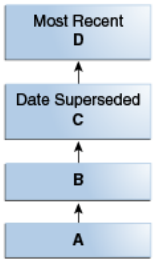
To step through an example of creating this type of link, see Renditions Link Example.

18.2.2 Supersedes

The predefined Supersedes relationship is based on the Chained List Class. It enables a user to create a hierarchical chain of content items where each item in the list is superseded by another item. One example is a subject-to-review content item, which must be maintained with current information. The supersede type causes the previous content item to become obsolete.

A supersedes relationship creates a hierarchy chain between items. The supersedes relationship is special because it enables a user to harness the disposition processing to handle superseded items. This type of relationship is created by anyone in the RecordsGroup security group to link an item superseding another.

Figure 18-2 Supersedes Links



The Supersedes relationship can be set on any item in the chained list, but is typically set on the most recent. The supersede date is set on the item that was superseded, not on the superseding item. Only the most recent version is shown in the Links area on the Content Information page; not all revisions are shown. The most recent item that superseded another item is at the top of the chained list.

For example, a monthly report for April (A) will be superseded by a report in May (B) that is later superseded by a report in June (C), and so on. This figure shows A was superseded by B, which was superseded in turn by C, which was superseded by D. Item D is the most recent record. The date superseded is set on the previously active record, which in this scenario is item C. To step through an example of creating this type of relationship, see Superseded Link Example.

18.2.3 Supporting Content

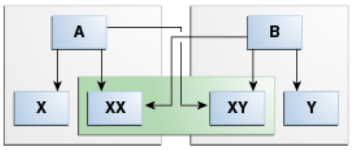
The predefined Supporting Content type is based on the Supporting Content Class. There is one main item (the parent) that has several subordinate, supporting items (the children). Supporting content links are based on the premise that a supporting content child can have multiple parent items they support. However, there can be only one parent to multiple child items. A supporting content relationship type can create a single parent-multiple children hierarchy between items.

This type of relationship can be created by anyone in the RecordsGroup security group to link an item to other items supporting the initial parent item in some way. For example, an image can be linked to a text file describing the printing requirements of that image. The supporting content type of relationship for an item with embedded content can also be used.

This relationship is convenient for linking portions of website content, such as an HTML document with placeholders to images, sound files, or video files. To create a parent-child

type of relationship between items crossing usage reference boundaries, the supporting content type can accommodate tracking the item relationships. A single image might be used in multiple parent documents, for instance, and a single document might contain multiple images.

Figure 18-3 Supporting Content Links



For example, a Word document (A) may have embedded content such as a spreadsheet (X) and a graphic (XX). Another document (B) may use some of the first document's content.

Figure 18-3 shows A and B are the only parent items. Item A has children X, XX, and XY. Item B has children XX, XY, and Y. Both child items XX and XY have multiple parents, A and B. To step through an example of creating this type of link, see Supporting Content Link Example.

18.2.4 Cross-Reference

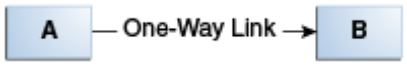
The predefined Cross-Reference relationship is based on the Cross-Reference Class. It is essentially a pointer from one item to another. This type of link can be created by anyone in the RecordsGroup security group to link items that reference each other. The link can be unidirectional (going one way only) or bidirectional (or reciprocal, going both ways).

To step through examples of creating these types of link, see One-Way Cross-Reference Link Example and Reciprocal Cross-Reference Link Example.

18.2.4.1 Unidirectional Links

In this example, A is linked to B. On the content information page for A, item A indicates a cross-reference relationship to B. On the content information page for B, item B indicates it is cross-referenced by a relationship to A.

Figure 18-4 One-Direction Cross-Reference Relationship

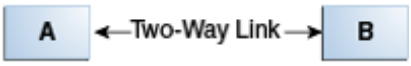


To step through an example of creating this type of relationship, see One-Way Cross-Reference Link Example.

18.2.4.2 Bidirectional (Reciprocal) Relationships

In the previous example, A points to B and vice versa. Item A is cross-referenced to B, and B is cross-referenced to A. When a reciprocal relationship is created from A to B, a cross-reference relationship is automatically created from B to A.

Figure 18-5 Both Directions (Reciprocal) Cross-Reference Relationship



To step through an example of creating this type of relationship, see Reciprocal Cross-Reference Link Example.

18.3 Linking Methods

There are two basic methods of creating relationships:

- Creating a relationship from one item to another item: If a relationship is created from an item in the system to another, existing item in the system, the search page can be used during the linking process to access the existing item and link to it. For details see Linking to an Existing Item.
- Creating a relationship from an existing item to a new item: If a relationship is added from an item in the system to a new item, use the content check-in page during the linking process to create the new item. For details see Linking to a New Item.

> **Note:**
>
> When items are deleted, all corresponding relationships are deleted except in the case when a superseded item is in the midst of disposition processing. A "dangling link" exists until the superseded item completes its disposition process then the relationships are deleted.

18.3.1 Relationship Classes

Each relationship type is based on a class definition of the relationship. There are four types of classes:

- Peer-to-Peer Class
- Chained List Class
- Supporting Content Class
- Cross-Reference Class

18.3.1.1 Peer-to-Peer Class

The peer-to-peer class represents a relationship between content where none of the items is more important than the other. There is no master or parent item. A typical example would be

different renditions of a document (for example, Word, PDF, or thumbnail image). The relationship is a many-to-many (m:n) relationship between peer items. Many content items (m) can have many relationships to other content items (n).

The system comes with the predefined Renditions relationship type based on the peer-to-peer class. For more information, see Renditions.

18.3.1.2 Chained List Class

The chained list class represents a relationship between content where the individual items are interconnected in series, thus creating a chain of linked items. An example would be incremental versions of items that supersede each other, where a user starts out with the first version, links the second version, links the third version, and so on. The latest linked item may supersede all previous items, but it does not need to. The relationship is a one-to-many (1:m) relationship between the superseding item and its superseded items. There can be one (1) content item that has superseded many (m) content items.

The chained list class is comparable to the revisions concept within Oracle WebCenter Content, but operates at a different level. Chained lists span multiple content items, whereas revision lists are for individual content items only.

Predefined types are available based on the chained list class.

18.3.1.3 Supporting Content Class

The supporting content class represents a relationship between content where there is one main item (the parent) that has several subordinate, supporting items (the children). Typical examples would be documents containing embedded images, or web files with placeholders to external images, sound files, or video clips. The parent item then links to the embedded or external supporting files (children), each of which is checked into the repository as a separate item.

The relationship is a one-to-many (1:m) parent-child relationship between one main item and its supporting items. There can be one (1) parent content item that has many (m) supporting content items. Even though there can only be one parent item in this relationship, child items can belong to multiple parents and reside in other sets of supporting content relationships. A child item can be the supporting content of many parents, but only one parent item can be supported by child items.

Predefined types are available based on the supporting content class. For more information, see Supporting Content.

18.3.1.4 Cross-Reference Class

The cross-reference class represents a one-to-one relationship between a pair of content items. The relationship is a cross-reference pointing a content item to another content item. The relationship can be unidirectional (pointing in one direction) or bidirectional (pointing in both directions, or reciprocal). A typical example would be a document containing a reference to another document, where these documents are linked together.

Predefined types are available based on the cross-reference class. For more information, see Cross-Reference.

18.4 Managing Related Content

The following tasks are involved in managing links:

- Adding a Custom Relation Type
- Editing a Custom Relation Type
- Deleting a Custom Link Type
- Linking Items
- Unlinking an Item

18.4.1 Adding a Custom Relation Type

You must use one of the predefined classes for this task.

> **Note:**
>
> The Admin.ConfigureLinkTypes right is required to perform this action. This right is assigned by default to the Records Administrator role.

1. Choose **Records** then **Configure** from the top menu.
2. Choose **Retention** then **Related Content Types**.
3. On the Configure Link Types page, click **Add Related Content Type**.
4. On the Add or Edit Related Content Type page, enter a name.
5. (Optional) Enter a destination.
6. Select a type from the **Class** list. For more information about classes, see Relationship Classes.
7. Click **Add**.

   The new type is added.

18.4.2 Editing a Custom Relation Type

To edit the name or destination of a custom type:

1. Choose **Records** then **Configure** from the top menu.
2. Choose **Retention** then **Related Content Types**.
3. On the Configure Link Types page, click **Add Related Content Type**.
4. On the Add or Edit Related Content Type page, in the **Actions** menu for the custom link to edit, choose **Edit**.
5. If required, edit the name and enter or edit a destination.
6. Click **Submit Update**.

   The type is updated on the Configure Link Types page.

18.4.3 Deleting a Custom Link Type

You cannot delete built-in types (System =Yes). If a custom type is in use, it cannot be deleted until it is removed from use. For further details, see Unlinking an Item. When deleting a custom type, this deletes the type definition, but does not delete any of the associated items.

> **Note:**
>
> The Admin.ConfigureLinkTypes right is required to perform this action. This right is assigned by default to the Records Administrator role.

1. Choose **Records** then **Configure** from the top menu.
2. Choose **Retention** then **Related Content Types**.
3. On the Configure Link Types page, choose **Delete** from the **Actions** menu for the link type to delete.

   You are prompted to confirm the action.
4. Click **OK**.

   The link type is deleted from the Configure Link Types page.

18.4.4 Linking Items

Links can be made to a new item or to an existing item. A link can be made from items in the retention schedule to new items checked in, or an existing item found during searching:

- **Link New Item**: Opens the Content Check In Form so the user can check in a new item linked to an existing item.
- **Link Existing Item**: Opens the Search page so a user can search for the existing items to link to an existing item.

Users can also create a link to an item during checkin. The Content Relations field is available at the bottom of the check-in page. Use the **Browse** button next to that field to search for an item to link.

> **Note:**
>
> The maximum number of items that you can link using the Related Items component is limited by the XRELATEDCONTENTLIST value in the DOCMETA table, which determines the size of the column. The default is 2000.
>
> You must suspend the replication of WebCenter Content to other installations before modifying the XRELATEDCONTENTLIST value in the DOCMETA table.

18.4.4.1 Linking to a New Item

1. Access the item from which to link:
   - Browse the retention schedule and list items within a category or record folder.
   - Screen Content for the item if you have the Records Administrator privilege.
   - Search for an item to link.
2. From the Retention Schedule, Screening Results, or Search Results page, choose the relationship type from the item's **Actions** menu.
3. In the Page menu of the link page, choose **Link** then **Link New Item.**

   The Content Check In Form opens.
4. Check in the new item to which to link.

18.4.4.2 Linking to an Existing Item

1. Access the item for linking:
   - Browse the retention schedule and list items within a retention category or record folder.
   - Screen Content for the item if you have the Records Administrator privilege.
   - Search for an item to link.
2. From the Retention Schedule, Screening Results, or Search Results page, select the relationship type from the item's **Actions** menu.
3. Click the **Add Link** action for the type of link to make.

   The link page for the link type opens.
4. In the menu of the link page, choose **Link** then **Link Existing Item**.

   The Advanced Search page opens.
5. Search for the item to which to link.

   A search results page opens with a Link column added.
6. Select the check box in the Link column next to the item or items to which to link.
7. From the Table menu, choose **Link** then **Link Selected Items**.

   The Link page for the type of link created opens, listing the item to which the link was established.

18.4.5 Unlinking an Item

There may be some compelling reason to remove a link, such as rerouting a link, or using a different type of link altogether. To unlink two linked items:

> **Note:**
>
> To unlink *destination links* such as Cross-Referenced By or Supported Content By, you must unlink from the content information page of the originating item. The destination links are the links appearing indented in the Links area of the content information page except for reciprocal cross-reference links. You can unlink from either link page in that case.

1. Navigate to the content information page of the item to unlink.
2. Click the links with a (+) to open the respective link page.
3. Choose **Unlink** from the item's **Actions** menu.

   A message opens asking for confirmation of removal of the link.
4. Click **OK**.

   The link page opens with the formerly linked content item no longer listed.

18.5 Link Examples

The following examples demonstrate how to create different types of links. The information in this section is restricted to users with the Records Administrator role:

- Enclosures Custom Link Types Example
- Renditions Link Example
- One-Way Cross-Reference Link Example
- Reciprocal Cross-Reference Link Example
- Superseded Link Example
- Supporting Content Link Example

18.5.1 Enclosures Custom Link Types Example

This example creates a link type with a custom name, and because it is a parent-child relationship, it also creates a destination link. The destination child link brings up any linked supporting items. This example creates a supporting content link types named `Enclosed by` with a destination link of `Enclosing Document`, and `Enclosure of` with a destination link called `Enclosures`.

1. Choose **Records** then **Configure**.
2. Choose **Retention** then **Related Content Types**.
3. On the Configure Link Types page, click **Add Related Content Type**.
4. On the Add or Edit Related Content Type page, enter the name `Enclosed By` for the link in the Name field.
5. Enter `Enclosing Document` in the Destination field.
6. Select the **Supporting Content** link type from the **Class** list.
7. Click **Add**.

The new link type is added to the Configure Link Types page.

8. Click **Add Related Content Type**.
9. On the Add or Edit Related Content Type page, enter the name `Enclosure of` for the link in the Name field.
10. Enter `Enclosures` in the Destination field.
11. Select the **Supporting Content** link type from the **Class** list.
12. Click **Add**.

    The new link type is added to the Configure Link Types page.

The new custom link names are shown in the Configure Link Types page. The Actions column is now populated with a menu for the custom link types, which are indicated by the System column being populated with the value No.

The custom link types are also available to users in the Links area of the content information page. They are also available for use in the Page menu of the search results page.

If links exist for a particular link type, a plus sign (+) is shown after the link type in the Content Information page.

An Enclosed By link to other content items is present for the current item. When a link is clicked, a list of the linked items is displayed.

18.5.2 Renditions Link Example

This example gives the basic steps for creating a renditions link between items. This example creates a rendition link from a newly checked in item to other newly checked in items. This example checks in a master graphics file called *Master PSD* and then checks in renditions, or different graphics formats of the same file (GIF, PNG, JPEG, BMP, and TIFF), as renditions links to the Master PSD file.

It is probably most convenient to link just after checking in an item because a user does not have to search or browse for the item.

1. Check in an item called `Master PSD`. Immediately after checking in, click the **Content Info** link available on the check-in confirmation page.
2. In the Links area of the content information page, click **Renditions**.

   The Renditions link page opens and is initially blank for the new and unlinked item.
3. In the Page menu, choose **Link** then **Link New Item**.
4. Check in an item called `GIF version` completing only required fields. After clicking **Check In**, the newly checked in and linked item is shown in the Renditions link page for the item.
5. Repeat linking new and checking in versions called `JPEG` and `TIFF`.

Click the **Info** icon and check the **Renditions** link for a rendition link. For any of the items on the Renditions link page, they all list each other in their own respective Renditions link pages. All items listed as a rendition link have a Renditions (+) indication on their content information pages.

18.5.3 One-Way Cross-Reference Link Example

This example creates a one-way cross-reference link. The one-way link points one item to another one. Item A (Disaster Recovery Procedures) is cross-referenced to item B (System Backup).

This example creates a one-way cross-reference between existing items. First search for the item to which to create links, and then search for the item or items to link. In this example, `Disaster Recovery Procedures` is linked to the existing `System Backup`. For the purposes of trying this example, create two items with these titles and then search for them.

1. Browse the retention schedule or search for an item to link, for this example, the item called `Disaster Recovery Procedures`.
2. From the Retention Schedule or Search Results page, click the **Info** icon.

   The content information page for the item opens.
3. In the Links area of the content information page, click **Cross-References from the listed links**.

   The Cross-References link page for the item opens and is initially blank.
4. In the Page menu of the Cross-References Link page, choose **Link** then **Link Existing Item**.

   The Search Results page for linking the item opens.
5. Enter the search criteria, and click **Search**.

   The Search Results page opens with a choice of items to link. The title indicates the item from which the user is linking. If the search criteria includes the item from which the user is linking, the check box is unavailable for selection. This prevents linking an item to itself.
6. In the Search Results page for linking, select the check box for the items to have links.
7. In the Page menu of the Search for Links page, choose **Link**.

   The items are linked, and the Cross-References page opens again with the ID and Titles of items linked as cross-references.
8. Now click the **Info** icon for a cross-referenced item to open the content information page. Scroll down to the Links area.

   The item from which we are linking has a (+) appearing after the Cross-Referenced By link.
9. Click the **Cross-Referenced By** link.

   The **System Backup: Cross-Referenced By** link page for the item opens.
10. Click the **Info** icon and access the content information page for the cross-referenced item.

    The item from which the link originated has a plus sign (+) appearing after the cross-references link.

18.5.4 Reciprocal Cross-Reference Link Example

This example creates a two-way link, meaning the linked items point to each other. This example creates a reciprocal cross-reference between existing items. First search for the item to which to create links, and then search for the item to link. Similar pages to those used to create a cross-reference link are used and so are not replicated here.

As in the previous example, Disaster Recovery Procedures is linked to the existing System Backup. For the purposes of trying this example, you can create two items with these titles and then search for the items. If you created links for the one-way example, unlink the items before proceeding with this example to view the same results as demonstrated for this example.

1. Browse the retention schedule or search for an item to link.
2. From the Retention Schedule or Search Results page, click the **Info** icon.

   The content information page for the item opens.
3. In the Links area of the content information page, click **Cross-References from the listed links**.

   The Cross-References link page for the item opens and is initially blank.
4. In the Page menu of the Cross-References Link page, choose **Link** then **Link Existing Item**.

   The Search Results page for linking the item opens.
5. Enter your search criteria, and click **Search**.

   The search results are displayed for you to choose items to link. The title indicates the item you are linking from. If your search criteria includes the item from which you are linking, the check box is unavailable for selection. This prevents linking an item to itself.
6. In the Search Results page for linking, select the check box for the items to which to create reciprocal links.
7. In the Page menu of the Search for links page, choose **Link** then **Link Reciprocal**.

   The items are linked, and the Cross-References page opens again with the ID and titles of items linked as cross-references.
8. Now click the **Info** icon for the cross-referenced item `System Backup` to open the content information page for the item which was just linked. Scroll down to the Links area. Notice the Cross-Reference and Cross-Referenced By links now indicate the reciprocal cross-reference links. Each Cross-References link now contains the plus (+) signs, and this appears for the content information pages of both items.
9. Click the **Cross-Referenced By** link.

   The Cross-Referenced By links page opens for the item.

You cannot perform any action from the Cross-Referenced By links page except viewing content information for any listed items. You must unlink the cross-referenced by items from their respective originating cross-references link pages; the same is true of Supported Content By or other indented (destination) links.

18.5.5 Superseded Link Example

This example demonstrates creating a superseded link. Because subject-to-review content must be kept up-to-date, this example demonstrates superseding items that are subject to review. You can supersede items not subject to review as well. This example locates a subject-to-review item, accesses the supersedes link, and checks in a new item that supersedes the existing one.

The supersedes link is a special type of link allowing you to take advantage of disposition processing to handle the superseded items. You can set up a category to have disposition processing rules such as **Destroy AFTER superseded** or **Archive AFTER superseded**. The supersede linking does not itself process superseded items; you must file the item into a category whose disposition instructions include handling superseded states.

The most likely scenario for superseding is to link a new item to an existing item. When new content is linked superseded to existing content, the existing content becomes obsolete and is marked as superseded automatically. The superseded and obsolete dates are populated for you on the content information page of the superseded item.

The current reigning content is always at the top of the list of superseded content. The superseded content is all underneath the current one, and (Superseded) is indicated parenthetically after each superseded item. The superseded items are displayed in the order the superseding occurred, starting with the first at the bottom of the list.

Of course, you do not have to file content that might be superseded into categories containing disposition instructions explicit to superseded. Multiple versions of superseded content can exist; their respective disposition instructions may just involve a retention period and then a destruction.

To step through this example, create a subject-to-review item called `Status Report`. If you have a non-production instance containing a subject-to-review category with disposition instructions for handling superseded content states, file the item into that category. Create another document called `new status report` but do not check it in before the example. It will be checked in during the example.

To try out this example:

1. Search for an item to link that is subject to review, for this example, an item called `Status Report`.
2. From the search results page, choose **Add Link (Supersedes)** from the **Actions** menu of the item to link.

   The Supersedes link page opens for the item.
3. Choose **Link** then **Link New Item** on the Page menu.

   The Content Check In Form opens.
4. Check in the document you created called `New Status Report` as a subject-to-review item into a category whose disposition instructions include actions to handle a superseded state.

   The Supersedes link page opens again with the superseded content and its linked item shown. The originating content that was superseded is now in the list, with its superior item now listed above it.

Because the disposition instruction of the Status Report is set to destroy when superseded, the administrator responsible for the item will receive a notification there is a pending event for the administrator to process (destroying the superseded item).

18.5.6 Supporting Content Link Example

This example demonstrates creating a supporting content link between existing content items.

1. Search for an item to link, for this example, an item called `Main HTML Home Page`.
2. From the Search Results page, choose **Add Link (Supporting Content)** from the item **Actions** menu.

   The Supporting Content link page opens for the existing item called `Main HTML Home Page`.
3. In the Page menu, choose **Link** then **Link Existing Item**.

   The Advanced Search page opens with the ID of the item in the title.
4. Enter your search criteria, and click **Search**.

   The Search Results page opens.
5. Select the item to link as supporting content by selecting the check box for the item.
6. In the Page menu, choose **Link**.

   The Supporting Content Link page for the item opens again, listing the now linked items.
7. Repeat the supporting link process for the parent item `Annual Corporate Report Brochure` and link it to the child item `Corporate Logo`, as shown below.
8. Click the **Info** icon to access the content information page for the Corporate Logo Image child item.

   The Supported Content By links indicates there are links present because there is a plus sign.
9. Click the **Supported Content By** link to show the link page for the child item.

   The Supported Content By indicates the content the item supports. The child item `Corporate Logo` shows its multiple parents.

19

Managing the Records System

Managing an Oracle WebCenter Content: Records system includes scheduling tasks for completion at other times, creating reports as needed, creating custom scripts, monitoring system performance, monitoring the audit trail and archiving information. This chapter describes those common tasks.
This chapter discusses the following topics:

19.1 Scheduling Tasks

It is possible to set up a schedule to perform retention-related tasks at times that are more convenient for your environment. This chapter discusses scheduling tasks that can be performed at a later time. It covers the following topics:

Some of the tasks performed may involve large sets of content. Tasks such as processing retention assignments, performing archives, or customizing metadata may interfere with normal daily operations or put a heavy load on the system, which is undesirable during regular business hours.

With the scheduling feature tasks can be set to be performed at a later time, during off-peak times on the system. Freezes can also be scheduled to be performed at specific times.

The following topics are discussed in this section:

19.1.1 Scheduling Screening Reports

To schedule a screening report, first screen for information using the screening function. Select the source then choose the scheduling criteria such as name for the report, start date, indication if it will recur, and the recurrence frequency for the report. You can also subscribe to the report and be notified when the report is generated.

The screening report is then put in the queue of actions to be performed. All scheduled screening reports are generated daily at midnight by default.

19.1.2 Editing Recurring Screening Reports

To edit a recurring scheduled screening report:

1. Choose **Records** then **Scheduled** then **Screening Reports**.
2. On the Scheduled Screening Reports page, choose an **Edit** option in the **Actions** menu of the screening report to modify:
   - **Edit schedule**: Change the scheduling criteria for the job. After clicking, the Edit Recurring Report Schedule page opens. Change any schedule details and click **Submit Update** when done.
   - **Edit criteria**: Used to change the criteria used for screening. After clicking, the Screen for Topic page opens. Choose the new criteria for screening and click **Submit Update**.
   - **Edit subscription**: If the user is subscribed to the report, that subscription can be changed to include other users or a group of users. Choose the new users and click **OK** when done.

19.1.3 Viewing Recurring Screening Report History

To view the history of recurring scheduled screening reports:

1. Choose **Records** then **Scheduled** then **Scheduled Screening Reports**.
2. On the Scheduled Screening Reports page, choose **Report History** in the **Actions** menu of the recurring screening report whose history will be viewed.
3. To view a report, click its link in the Name column.

19.1.4 Scheduling and Unscheduling Freezes

Use this procedure to schedule a recurring freeze of selected items. This optional feature will freeze any new items that match the search criteria specified from the search page.

To unschedule a freeze, select **Records** then **Scheduled** then **Freezes**. Select Unschedule from the **Action** menu of the scheduled freeze.

1. Search for the items to include in the scheduled recurring freeze.
2. On the Search Results page, choose **Edit** then **Freeze All Search Results** from the Table menu.
3. In the open dialog, select the freeze reason from the list.
4. Enter a freeze reason (optional).
5. Select **Schedule Recurring Freeze Inclusion** then click **OK**.

19.1.5 Viewing Scheduled Job Information

To view a list of all scheduled jobs (reports, freezes, and any other Oracle WebCenter Content scheduled jobs):

1. Choose **Administration** then **Scheduled Jobs Administration**. Choose **Active Scheduled Jobs**.

2. The Scheduled Jobs Listing page opens, showing all scheduled jobs.
3. To view details about a particular job, click the **Info** icon for that job. To edit details about the scheduled job, select **Edit** from the **Actions** menu for a particular item.
4. The Job Information page/Edit Job Information page opens. This page can be used to edit job details such as priority, the type of job, and so forth.

19.2 Using Performance Monitoring

Performance monitoring can be enabled to check the status of batch processing, service calls, and other system information.

Several default numbers have been set as a starting point for monitoring. Actual performance variations will depend on the hardware used at the site and other variables such as total amount of content and software in use.

The frequency with which you need to update statistics depends on how quickly the data is changing. Typically, statistics should be updated when the number of new items since the last update is greater than ten percent of the number of items when the statistics were last updated.

If a large amount of disposition processing is being done (for example, at the end of the calendar year for organizations that synchronize dispositions on the calendar), you should update statistics at the end of the week rather than wait for a particular percentage of data updates.

Performance monitoring statistics are written to a database table and can be accessed later.

This section discusses the following topics:

- Enabling Performance Monitoring
- Checking Performance Results
- Viewing Performance Alerts and Details

19.2.1 Enabling Performance Monitoring

To use performance monitoring:

1. Choose **Records** then **Audit**. Choose **Configure** then **Performance Monitoring**.
2. On the Configure Performance Monitoring page, select the items to monitor and the time intervals for reports and alerts.
3. Click **Submit Update** when done.

19.2.2 Checking Performance Results

After enabling performance monitoring, current performance information can be checked using this procedure:

1. Choose **Records** then **Audit** then **Performance Monitoring**.
2. On the Performance Processing Results page, choose the type of information to view by clicking the tab at the top of the body section of the page:
    - **Performance Processing**: This page contains a summary of requests processed, total items processed, total number of queries run, total time to run queries, total time

to validate data, total service request parse time and total service request time per each source. Averages for these are also included.

- **Report by Batch**: This page contains a summary of batches/items pending, processed, and failed with a total for each source. If an item has failed, a batch file is created that can be re-run. Click on any value in a column to open a page showing details about that item and to access the option to re-run the batch.
- **Report by Item**: This page contains the details per batch for a particular source, status or batch type as well as totals. The detail page for the item contains the batch type, start time, completed time, elapsed time, and number of items processed for each batch.

19.2.3 Viewing Performance Alerts and Details

If any performance activities exceed the limits set on the Configure Performance Monitoring page, a message is displayed automatically when you log in to the system.

Click any link on the message to see details about the specific alert. For example, a detail page opens when the first alert message is clicked. Click any link to show details about the specific items that caused the alert.

19.3 Using Custom Scripts

Custom scripts can be created using Idoc Script, a proprietary scripting language. This functionality is enabled by default when the DoD Configuration component is enabled.

Custom scripting can be disabled by deselecting **Enable Custom Script** in the DoD Config section of the Configure Retention Settings page. To access that page choose **Records** then **Configure** then **Settings**.

When enabled, new content fields are available that allow you to define which scripts will apply to a folder or category.

> **Note:**
>
> You must have a thorough understanding of Idoc Script to use this feature. The software does not validate the script. You are responsible for creating usable scripts. For details about Idoc Script and its use, see *Developing with Oracle WebCenter Content*.

Two types of scripts can be created using the Custom Script functionality:

- Security scripts, which allow users with the Records Administrator role to define and manage access control to content.
- Custom Notification scripts, which notify users of events. One custom script is provided, which notifies a list of reviewers when items are due for destruction after being superseded. Notification is sent in one consolidated email when batches are run. Additional scripts can be created.

Scripts can be applied at a category or folder level but content in the category or folder does not automatically inherit the script. Consider the following scenario:

- A custom script is created to prevent user A from viewing content.
- A folder is created and the custom script is applied to it.
- An item is checked in by user B to the folder.
- User A browses through the folder and sees the title of the item checked in by user B. However, if user A tries to view the actual item, an error is returned.

To prevent user A from even seeing the title of the item, the security script must be set so items included in the object (category or folder) explicitly inherit the attributes of the script. For example, to set inheritance in a category, the following variable would be set in the `config.cfg` file:

```
RecordsMetaInheritFromCategory=dSecurityScripts:xSecurityScripts
```

To set inheritance for a folder, use the `RecordsMetaInheritFromFolder` variable.

> **Note:**
>
> Custom scripts comply with the DoD 5015.2 specification, chapter 4.19 and chapter 4.20.

This section discusses the following topics:

- Creating or Editing Scripts
- Deleting a Custom Script
- Viewing Script Information

19.3.1 Creating or Editing Scripts

> **Note:**
>
> Any custom Idoc Script that is entered is NOT verified for accuracy. You should have knowledge about Idoc Script and its uses before creating scripts.

To set up a script:

1. Choose **Records** then **Configure**.
2. Choose **Security** then **Custom Scripts**.
3. On the Configure Custom Script page, select the type of script to use (Notification or Security) by clicking the tab for the script type.
   - To edit an existing script, choose **Edit** from the script's **Actions** menu.
   - To add a script, choose **Add** or **Edit** on the Custom Script Information page.
4. On the Create or Edit Custom Script page, add or edit the name for the script.
5. Add or edit the description for the script (optional).
6. Add or edit the Idoc code for the script. Note that the code is not verified for accuracy.

7. When finished adding a new script, click **Create**.

   When editing a script, click **Submit Update**.

   To reset the page without saving, click **Reset**.

19.3.2 Deleting a Custom Script

To delete a script:

1. Choose **Records** then **Configure**.
2. Choose **Security** then **Custom Scripts**.
3. On the Configure Custom Script page, select the type of script for deletion by clicking the tab for either a Notification or a Security script.
4. To delete the script, select the box next to the script name and choose **Delete** or **Delete Script** from the script's **Actions** menu. You can also choose **Delete** on the Custom Script Information page.

19.3.3 Viewing Script Information

To view a script's information:

1. Choose **Records** then **Configure**.
2. Choose **Security** then **Custom Scripts**.
3. On the Configure Custom Script page, select the type of script for viewing by clicking the tab for either a Notification or a Security script.
4. To view the script information, click the script name or choose **Script Information** from the script's **Actions** menu.

19.4 Using the Audit Trail

The audit trail is generated in the format specified by the Report Format setting on the Configure Report Settings page.

> **Note:**
>
> The Admin.Audit right is required to work with audit trails. This right is assigned by default to the Records Administrator role. Administrative privileges are required to check in the audit trail.

At certain points, the current audit trail can be cut off and archived and checked into the repository. This action can also be scheduled to occur on a regular basis. The audit trail must be cycled for growth reasons the same as other items. Be sure to check in the audit trail log on a regular basis to keep the file size smaller and the report generation time faster. Each current audit trail is generated from the time the system was installed or archived until the request to generate an audit trail.

An audit trail can be generated at any time. The columns within the audit trail correspond directly with the fields you can use to search within the Search Audit Trail page.

If the generated file is in PDF format, Adobe Acrobat version 6.0 or later is required to view it.

Several tasks are involved in managing Audit Trails:

- Configuring the Audit Trail
- Specifying Metadata Fields to Audit
- Searching within the Audit Trail
- Setting Default Metadata for Checking In Audit Trails
- Checking In and Archiving the Audit Trail
- Searching an Archived Audit Trail
- Viewing an Archived Audit Trail
- Creating an Audit Trail Report

19.4.1 Configuring the Audit Trail

The configuration on the Configure Audit page determines the administrator and user actions recorded for an audit trail.

> **Note:**
>
> The Admin.Audit right is required to perform this action. This right is assigned by default to the Records Administrator role.

To configure an audit trail:

1. Choose **Records** then **Audit**.
2. Choose **Configure** then **Audit Trail**.
3. On the Configure Audit page, select the boxes for the actions to audit for each entity.
4. Click **Submit Update**.

   A message indicates configuring the audit was successful. The next time the audit trail is generated, the trail reflects the chosen selections.
5. Click **OK**.

   The Configure Audit page opens again with the updated settings.

> **Note:**
>
> If actions are deselected for objects, the actions are *not* captured by the audit trail. It is recommended you leave all settings selected and use the Search Audit Trail page to narrow down searches of the audit trail. If transactions are heavy and the audit log grows too large too fast, you might want to consider turning off capturing browsing actions to manage the audit trail size.

19.4.1.1 Configure Audit Page

> **Important:**
>
> The Admin.Audit right is required to use this screen. This right is assigned by default to the ‘rmaadmin’ role.

By default, all options are selected when you first access the Configure Audit page. To access this page, select **Records** > **Audit** > **Configure** > **Audit Trail**.

> **Note:**
>
> The Edit Metadata column is only visible if the Log Metadata Changes option is enabled on the Configure Retention Administration Page.

Audited Objects and Features	Actions Recorded
Series Category Folder Period Trigger Custom Direct Trigger Indirect Trigger Supplemental Marking Security Classification Configuration Record or Content Freeze User Groups User Accounts Indirect Trigger Date Custom Security Field Related Content Type Disposition Action Metadata Set	Select the check boxes for the actions you want recorded within the current audit trail: • **Delete**: All action of deleting items are recorded in the current audit trail. • **Edit**: All actions of editing items are recorded in the current audit trail. • **Create**: All actions of creating items are recorded in the current audit trail. • **Retrieve**: All items that are retrieved are recorded in the audit trail. This means the information was viewed within an information page. • **Browse**: All browsing actions within the retention schedule are recorded in the current audit trail. • **Search**: All searching actions for items are recorded in the current audit trail. Screening is also captured by the Search action. • **Edit Metadata**: All metadata changes for items, categories, folders, and series are recorded in the current audit trail. Not only is the changed status recorded, but also what the change entails (old and new field values). This column is only visible if the Log Metadata Changes option is enabled on the Configure Retention Administration Page. **Note:** The User Accounts column represents records users and is not to be confused with the accounts-based security model within Universal Content Management. The Configure Audit User Accounts option tracks users and not document accounts. The User Groups options tracks users assigned to an alias group.
Submit Update button	Submits your updates.
Reset button	Resets the page to the initial settings.

19.4.2 Specifying Metadata Fields to Audit

Use this procedure to specify which metadata fields should be included in the audit trail.

Note:

The Admin.SelectMeta right is required to perform this action. This right is assigned to the Records Administrator role by default.

1. Choose **Records** then **Audit**.
2. Choose **Configure** then **Audit Fields**.
3. On the Audit Fields page, select the boxes for the metadata field to include in the audit trail.

4. Click **Submit Update** when done.

Any changes take effect immediately without restarting the system.

19.4.3 Searching within the Audit Trail

Use this procedure to further refine a search within the current audit trail. For example, you can search for all delete actions, or all delete actions by a particular user, or all actions by a particular user, and so on.

When sorting the audit trail using Oracle DB, the output depends on the type of sort being performed. When sorting with Fulltext Search, sorting is case-sensitive, meaning that upper case items (capitalized items) will appear first in a list. When sorting with Oracle Text Search, a case-insensitive search is performed.

> **Note:**
>
> The Admin.Audit right is required to perform this action. This right is assigned by default to the Records Administrator role.

1. Choose **Records** then **Audit** then **Search Audit Trail**.
2. On the Search Audit Trail page, make the selections to narrow the search. As much or as little detail can be included. To adjust the scope (narrow or widen) of the search, use the Boolean operators before each field.
3. Click **Search**.

   The search results appear in the format specified by the Report Format setting on the Configure Report Settings page.

19.4.4 Setting Default Metadata for Checking In Audit Trails

Setting the default metadata is useful for setting similar check-in attributes. You *must* set the default metadata before checking in an audit trail for the first time. This is a required step during the setup of the software.

> **Note:**
>
> The Admin.Audit right is required to perform this action. This right is assigned by default to the Records Administrator role.

To set the default metadata:

1. Choose **Records** then **Audit** then **Checked-in Audit Entries**.
2. On the Checked-in Audit Entries page, click the **Default Metadata for Checked-In Audit Entries** link.
3. On the Default Metadata for Checked-In Audit Entries page, make selections reflecting the metadata most commonly used when checking in an archived audit trail. When finished, click **Submit Update**.

A message appears saying the default metadata has been updated successfully.

4. Click **OK**.

19.4.5 Checking In and Archiving the Audit Trail

A user must have performed at least one action while logged into the system to generate an audit trail entry. If an empty audit trail is submitted for check-in, a message is displayed indicating there are no entries in the audit trail. Before checking in an audit trail for the first time, set the default metadata for the checkin.

> **Note:**
>
> The Admin.Audit right is required to perform this action. This right is assigned by default to the Records Administrator role.

1. Choose **Records** then **Audit** then **Checked-in Audit Entries**.
2. On the Checked-in Audit Entries page, specify the date and time to cut off the audit trail in the Date box, and click **Archive**.

   The check-in confirmation page opens. The content ID of the checked-in audit trail is `AUDITLOGARCHIVE`. Every time it is checked in, a new revision is generated.
3. Click **Content Info** to view the information about the archived audit log.

   The Content Information page opens.
4. To view the audit log just checked in, click the **Web Location** or the **Native File** in the Links area of the Content Information page.

19.4.6 Searching an Archived Audit Trail

To search for all checked in and archived audit trails:

Prerequisites

- Checking In and Archiving the Audit Trail

> **Note:**
>
> The Admin.Audit right is required to perform this action. This right is assigned by default to the Records Administrator role.

1. Choose **Records** then **Audit** then **Checked-in Audit Entries**.
2. On the Checked-in Audit Entries page, click **Search Audit Entries**.

   The results of the search appear in the search results page.
3. From the search results page, click options in the **Query Actions** list to search within the results and save the search.

19.4.7 Viewing an Archived Audit Trail

To view an archived audit log from the search results page, do one of the following:

- Click the ID (quickest method)
- Click the **Info** icon then click the PDF links on the Content Information page.

19.4.8 Creating an Audit Trail Report

An audit trail report is automatically generated in the format specified by the Report Format setting on the Configure Report Settings page. If the generated file is in PDF format, Adobe Acrobat version 6.0 or later is required to view it.

19.5 Using Default Reports

Reports are initially configured through menu options on the Configure Report Settings page. During configuration a profile can be specified to be used when creating or updating a report template, and a profile to be used when creating or updating a report. A report format can also be chosen and if the report or template should be included when performing searches.

> **Note:**
>
> If barcode labels will be printed, specify PDF for the report format. Labels will display in HTML output but they can only be printed correctly using the PDF option.

To configure default options to be used with all reports:

1. Choose **Records** then **Configure**.
2. Choose **Reports** then **Settings**.
3. On the Configure Report Settings page, choose the report template profile from the option list or use the default profile provided.
4. Choose the profile to use when creating or updating a report.
5. Choose the report format to use. Options include HTML, PDF, RTF, or XLS. Note that if barcode labels are to be printed, this must be set to PDF.
6. Check the box to exclude all report templates during search operations.
7. Check the box to exclude all checked-in reports during search operations.
8. When finished, click **Submit Update**.

19.5.1 User and Group Reports

After creating users and alias groups, and assigning management roles and rights to users, reports can be generated to view at a glance which users and alias groups have access to the system. The following reports are available:

- User Report
- User Barcode Reports
- User Roles Report
- Group Report
- Group-User Report

Reports are generated in the format specified by the setting on the user's profile page. To see the user format that is specified, click the user name in the top right corner of the screen and the User Profile page opens. If the system format is used, that usage is specified on the Configure Report Settings page.

If the generated report file is in PDF format, Adobe Acrobat version 6.0 or later is required to view it.

To generate reports, choose **Records** then **Reports** then the report type.

> **Note:**
>
> The Admin.Reports right is required to produce any reports. This right is assigned by default to the Records Administrator role. The Admin role is also required.

19.5.1.1 User Report

A list can be generated of all users who have access to the system as well as a barcode list for the users. A report can also be created that can be used to produce barcode labels. The users and the bar codes assigned to them are defined in User Admin utility. This report lists overview information for each user.

Column	Description
User Name	The name of the user as entered in the User Admin utility.
Full Name	The full name of the user as entered in the User Admin utility.
E-mail Address	The email address of the user.
Creation Date	The date and time the user was created in the User Admin utility.
Change Date	The date and time the user information was last modified.
Supplemental	Any supplemental markings assigned to a user.
Security Classification	The classification assigned to the user.
Alternate Reviewer	The alternate reviewer for this user.
Barcode	The barcode designation for the user.

19.5.1.2 User Barcode Reports

A report can be generated that lists barcode information and another type that can be used to produce barcode labels. The users are defined in the User Admin utility then assigned rights and roles.

View barcode reports using HTML but print reports using PDF in order to ensure proper formatting.

19.5.1.3 User Roles Report

Use this report to view a list of all users and their assigned roles. The output of the report may not show all data for all roles. The output is dependent on the user who is generating the report and the permissions given to that user.

Column	Description
User	The user name of the user as entered in the User Admin utility.
Roles	The roles assigned to the user.

19.5.1.4 Group Report

Use the All Groups report to view a list of all aliases defined for the system.

Column	Description
Group Name	Lists all alias groups defined in the User Admin utility.
Description	A short description of each alias group.

19.5.1.5 Group-User Report

Use this report to view a list of all users and groups (aliases) currently defined for access. The users and groups (aliases) are assigned in the User Admin utility.

Column	Description
Group	Lists all alias groups defined in the User Admin utility.
User	Lists every user assigned to an alias group.

19.5.2 Content and Physical Item Reports

Several default reports and templates are provided with the product. These reports are available in a variety of locations within the software such as search result page, Content Information pages, and so on. The type of reports depend on the configuration of the system and what components have been enabled.

This section describes how to generate content reports using the default templates provided. For information about creating custom reports, see *Developing with Oracle WebCenter Content*.

The following types of reports can be produced:

- Internal Item Detail Report: This report shows details about one item or about a group of items if several items are selected for use for the report. An external detail report is similar to this report, but it includes the bar code for the item as well as other information that pertains only to external items.
- Search Results Report: This report shows basic information about items such as content ID and author.
- Records Destruction Certificate Report: This report shows those items that are scheduled for destruction and which should be removed from the warehouse.

The creation of new reports is composed of two steps: finding the information for the report then choosing the appropriate report option.

1. Use searching or screening to find the information.
2. Use one of the following methods to create a report for an individual item:
   - Click the **Info** icon for the item. On the item's Content Information page, choose **Create Reports** then the type of report.
   - On the Search Results page, select the check box for an item. Choose **Create Reports** then **Selected Items** then the type of report.
3. To create a report for multiple items, select the check boxes of the items then choose **Create Reports** then **Selected Items** then the type of report.
4. To create a report for all items on the page (such as all search results), choose **Create Reports** then **Full Results** then the type of report.

19.6 Archiving and Transferring Information

If an environment is set up on one computer (including a retention schedule, security scheme, and so on), you may want to copy this configuration information to another computer, for example, from a development system to a production system or a mirrored site. This can be done using built-in archive import and export features.

You can also import and export records, folders, and metadata in XML format by creating a XML Standard Definition (XSD). XSD is a an XML schema language used to define the structure of an XML document. The XSD file is created to make the file usable in the Records system. This allows the content from the system to be imported into a third-party system using a different archive file format or to export data from another system and import it into the system.

This functionality is compliant with the DoD 5015.2 specification that requires the ability to create different XSD schemas.

> **Note:**
>
> When using the import/export process, make sure the instance to which you are importing has the same metadata fields, security groups, and accounts as the instance where the export is originating from. Errors can result if there are mismatches.

This section discusses the following topics:

- The Archive Process
- Managing Imports and Exports
- XSD Data Transfer

19.6.1 The Archive Process

The archive process is used to back up or restore a retention schedule and other configuration settings. It is not used to archive copies of content. For details about archiving content, see *Administering Oracle WebCenter Content*.

Note that if you import an archive from a 10g version of the software to the 11g version that includes a Related Content table, the import must be done in two steps. First import the content items in an archive. Then import the Related Content table.

The export feature copies a variety of configuration settings to a separate *.hda* file that can be imported into another instance or stored in a safe location for backup purposes. The *.hda* file is a plain text, serialized data file that can be opened in any text editor.

Retention Schedule objects should be imported before importing other content. Content Server content should be imported before importing the content-related objects.

> **Note:**
>
> For details, see Archive Import/Export Rights and Permissions.

The archive export and import features enable exporting and importing of the following items:

- Supplemental markings
- Security classifications, also known as Classified Markings
- Custom categories metadata and custom folder metadata
- Custom security fields, also known as Custom Supplemental Markings
- Periods
- Triggers
- Retention schedules
- Dispositions history: a log of all actions that have been performed
- Custom disposition actions
- Freezes
- Recurring scheduled tasks
- Classification guides and classification topics. These are only available if the ClassifiedEnhancements component is enabled.
- PCM location types
- PCM storage space definitions
- Custom PCM metadata
- Reservations

Note the following considerations when using imports and exports:

- When using PCM, the export feature copies the space management definitions (the setup and hierarchy of warehouses, rooms, and so on) but none of the metadata of the items stored at those locations is archived.
- When importing an archive, existing items can be overwritten or can be left unchanged.

- Set the default archive metadata format by choosing **Records** then **Configure** then **Settings** from the Top menu. The Configure Retention Settings page opens. Expand the General section and select the metadata format from the list.
- When custom category metadata fields or custom folder metadata fields are imported, the order of the fields is not updated. Restart the Content Server after importing custom fields.
- The disposition history is not updated. Only new dispositions are imported.
- The export feature copies the retention schedule definition (that is, the defined hierarchy) and disposition instructions, not the items within the retention schedule.
- If an additional component is enabled, there may be additional items available for export.

> **Note:**
>
> If your organization uses additional security (ACLs) on your retention schedule, the import and export only includes items that can be accessed by the user performing the import or export. For example, if the person does not have ACL access to a particular category, that category is not imported or exported. A message is displayed during the import or export process if any objects are not processed due to ACL access. Make sure you have ACL access to all items to export and import.

19.6.1.1 Exporting Auxiliary Metadata Sets

> **Note:**
>
> You must have administrative privileges to add tables to the list of schema tables used.

When exporting an auxiliary metadata set, add the AuxiliaryMetadataSets and AuxiliaryMetadataSetDefs table to the list of schema tables used. Follow this procedure to add those tables:

1. Choose **Administration** then **Admin Applets** from the main menu.
2. Click **Configuration Manager**.
3. In the Configuration Manager applet, click the **Tables** tab.

   A Table List opens.
4. Click **Add Table**.
5. Highlight AuxiliaryMetadataSets and click **OK**.

   The Table list opens again.
6. Highlight AuxiliaryMetadataSetDefs and click **OK**.

   The Table list opens again.
7. Close the Configuration Manager.

After adding the MetadataSet tables to the list of tables, they become available in the list of tables that can be added from the Archiver.

19.6.1.2 The Export/Import Process

The process of importing and exporting content consists of three distinct parts.

1. First import or export a retention schedule and any of the objects in that schedule. This corresponds to the **Include Retention Schedules Plan** portion of the Export and Import pages.
2. Then import or export the content using the Oracle WebCenter Content Archiver. For details about using the Archiver, see *Administering Oracle WebCenter Content*.
3. After content has been imported or exported using the Archiver, import or export the Disposition History of related objects. This corresponds to the **Include Dispositions History** portion of the Export and Import pages.

19.6.1.3 Archive Import/Export Rights and Permissions

The following export rights are needed for specific objects. These rights are included by default with the Records Administrator role:

- Admin.RetentionSchedulesArchive right: to export a Retention Schedule.
- Admin.Triggers right: to export triggers.
- Admin.PerformActions right: to export Disposition Histories.
- Admin.RecordManager right: to export objects other than those mentioned previously.

The following import rights are needed for specific objects:

- Category.Edit, Folder.Edit, and Record.Edit rights: to import a Retention Schedule (because these objects are part of a Retention Schedule).
- Admin.Triggers right: to import triggers.
- Admin.PerformActions right: to import Disposition Histories.
- Admin.CustomDispositionActions right: to import Disposition Actions.
- Admin.RecordManager right: to import objects other than those mentioned previously.
- If ACL security is enabled, make sure you have access to all retention schedule components and objects to import.

19.6.2 Managing Imports and Exports

The following tasks are performed when importing or exporting archives:

- Exporting an Archive
- Importing an Archive
- Importing a Batch-Created Storage Hierarchy

19.6.2.1 Exporting an Archive

Use this procedure to export an archive that can be imported into another instance (located on the same or a separate system) or for backup purposes. Choose which items should be exported.

> **Note:**
>
> For details, see Archive Import/Export Rights and Permissions.

1. Choose **Records** then **Import/Export** then **Archives** from the top menu.
2. On the Import/Export Archive page, select all items to be included in the export.
3. Click **Export**.

   A download dialog appears.
4. To save the archive, click **Save**. Navigate to the location to save the file, and enter a file name.
5. Click **Save**.

   The file is saved to the specified location, and the Import/Export Archive page opens.

19.6.2.2 Importing an Archive

> **Note:**
>
> When using the import/export process, make sure the instance to which you are importing has the same metadata fields, security groups, and accounts as the instance where the export is originating from. Errors can result if there are mismatches.

Use this procedure to import an archive that was exported on another instance (located on the same or a separate system). Choose which items in the archive should be imported. The items to import must have been included in the export of the archive.

> **Note:**
>
> For details, see Archive Import/Export Rights and Permissions.

1. Choose **Records** then **Import/Export** then **Archives.**
2. On the Import/Export Archive page, select all items to be included in the import. Click **Attempt Update** to specify whether to update existing items or leave them untouched. If you do not have update checked and the imported item(s) already exist, an error may occur. Read the error message to determine the best course of action to pursue.

3. Click **Browse** next to Archive File to select the archive file (`.hda`) to import.
4. After selecting the file, click **Import**.

   The import adds all new items and updates any existing ones, if applicable. The results of the imported archive are tracked in the audit trail for the enabled actions.

If an error occurs, the error message indicates the number of items that failed, not necessarily the number of individual errors for all retention schedule components. If classified markings are imported, they should be reordered after importation.

19.6.2.3 Importing a Batch-Created Storage Hierarchy

> **Note:**
>
> For details, see Archive Import/Export Rights and Permissions.

Use this procedure to import a storage hierarchy definition file (*StorageImport.hda*) that was created using the batch storage creation feature.

1. Choose **Records** then **Import/Export** then **Archives** from the top menu**.**
2. On the Import/Export Archive page, make sure the **Include Storage** check box is selected. You do not have to unselect all the other items. They are ignored if none of them are included in the `StorageImport.hda` file.
3. Click **Browse** next to Archive File to select the `StorageImport.hda` archive file that was created when you batch-created the storage hierarchy.
4. After selecting the file, click **Import**.

   The import adds the storage hierarchy contained in the `StorageImport.hda` file to the existing storage space at the location specified in the `.hda` file.

19.6.3 XSD Data Transfer

XSD schemas can be used to manage records, folders, and content to comply with the DoD 5015.2 specification. Exporting and importing data using a format defined as XSD format (XML Schema Definition) conforms with standard transfer schema defaults.

The information must be mapped before proceeding with exporting or importing. After the correct mapping is in place, data can be imported and used. It can then later be transferred as needed to NARA or another system using the XSD schema for that site.

Important considerations should be evaluated before beginning the import and export process:

- Special Handling of <choice> Elements
- Required Fields on Import
- Target Namespace and Qualified Locals
- Configuring XSD for Importing and Exporting
- Exporting XSD Data
- Importing XSD Data

19.6.3.1 Special Handling of <choice> Elements

The <choice> element type allows only one of the elements contained in the selected group to be present within a containing element. This differs from an option list where one field can have multiple possible values.

A document whose data is being exported can only contain a value in one of the fields contained in the <xs:choice> group. This restriction determines which field to use when the XML file is generated for output. If more than one of the fields in the choice group contain a value, an error occurs and the export cannot finish because of ambiguity as to which field should be used.

The following example shows this type of <choice> list. In this example, an employee can be only one of the three types of employees (full-time, part-time, or contractor). So only one of the three corresponding fields can be contained in the <choice> element.

```
<xs:complexType name="employee">
 <xs:choice>
 <xs:element ref="full-time" />
 <xs:element ref="part-time" />
 <xs:element ref="contractor" />
 </xs:choice>
</xs:complexType>
```

19.6.3.2 Required Fields on Import

If your server has required fields, all of those fields must have a value set in order to perform an import. Mapping the required fields to an XML node provides the value. However, if any of the required fields are not mapped, a profile must be created that sets these values on import. If this is not done, the import fails.

19.6.3.3 Target Namespace and Qualified Locals

Explicitly declare a target namespace in the `.xsd` file and also specify that locally defined elements and locally defined attributes are qualified. The target namespace is specified by the `targetNamespace` attribute.

Local elements and attributes can be qualified globally by using the `elementFormDefault` and `attributeFormDefault` attributes on the schema element. They can be specified separately for each local declaration using the `form` attribute. Attribute values can be set to *unqualified* or *qualified*, to indicate if locally declared elements and attributes must be unqualified.

19.6.3.4 Configuring XSD for Importing and Exporting

Use this procedure to configure the schema definition for the export.

1. Choose **Records** then **Import/Export**.
2. Choose **Configure** then **Import/Export Schema**.
3. On the Configure Import/Export Schema page, click **Add** to create a schema definition to use for the export.
4. On the Create Import/Export Schema page, enter the necessary information and click **Browse** to find an archive file for use. When done, click **Create**.

   The Upload Confirmation page opens.

5. Choose **Configure Top Level Nodes** from the page menu.

   The Configure Top Level Schema Nodes page opens. *Top level nodes* are those that represent an entire object, such as a record or a folder.

6. Highlight the nodes to include in the list, using the left or right arrows to move or remove the node. Choose mapping options in the mapping section, choosing the appropriate type from the menu lists. Click **Save** when done.

7. Choose **Map Fields** from the page menu to map folder and content fields.

   The Configure Mappings page opens. Use this page to map XSD fields to the Records system metadata fields for both records and folders. These mappings will be used for both exporting and importing. The custom mapping at the bottom of the page is used to resolve ambiguity when two different objects that are defined in the same XSD reference a common sub-object that must be mapped to different fields. To add fields, click **Add** at the bottom of the page and enter the new custom field. To delete custom fields, click the delete icon (a red X). Click **Save** when done.

19.6.3.5 Exporting XSD Data

After configuring the data to be exported, you can proceed with the import or export process.

1. Choose **Records** then **Import/Export**.
2. Choose **Export with Schema**.
3. On the Export with Schema page, choose a schema name from the list.
4. Expand the existing archive batch names and select an archive batch name.
5. Click **Export**.

19.6.3.6 Importing XSD Data

Follow a similar procedure to import an archive using XSD mapping by choosing **Import with Schema** from the menu.

1. Choose **Records** then **Import/Export**.
2. Choose **Import with Schema**.
3. On the Import with Schema page, choose a schema name from the list.
4. Select an archive file by clicking **Browse** and navigating to the location where archives are located.
5. Click **Import**.

20
Using Federated Search and Freeze

This chapter describes how to use Federated Search to gather information needed for a discovery action and how to use Federated Freeze to freeze those items for Oracle WebCenter Content: Records.
This chapter discusses the following topics:

20.1 Understanding Federated Search and Freeze

Federation is a term used to describe the process of providing a single point of contact/entry for searching multiple disparate data sources. This is often used during the legal discovery process. For example, by using the Federated functionality with the Records system, a legal officer can search all repositories and catalogs for items pertaining to a legal matter. The search results then connect all the items together in one place in order to perform legal searches.

Federated search is most effective when used with the adapters that manage content on remote repositories.

> **Note:**
>
> Federated Search functionality is not visible until the RmaNoSecurity right is added to a role. This right is not added by default to any role and must be enabled for the functionality to be accessible. This right should not be treated lightly or granted indiscriminately.
>
> In addition, a system administrator role is needed to use this functionality.

20.2 Federated Searches

Federated Search is available when an external repository (an adapter) is installed.

As part of a discovery process, organizations might search for or freeze content across multiple repositories that are managed by adapters. Records uses external adapters to search metadata and full text of remote repository items. With this functionality, a user can:

- Create searches by sending the search criteria to the adapter. External adapters check periodically to see if there are searches pending, perform the searches, and return the search results. The adapters may perform the search in a delayed timeline, requiring users to wait for the search results to complete.

- Freeze the content returned from a completed scheduled search. While scheduled freezes are initiated immediately, the Records system performs the freeze in the background.
- View detailed information about a scheduled search or freeze.
- View search or freeze results.
- Delete a scheduled search or freeze.

This section discusses the following topics:

- Federated Search Query Builder
- Performing a Search

20.2.1 Federated Search Query Builder

To access the Federated Search Query Builder choose **Search** then **Global Search**. The following options are available:

- **Central Catalog Search** is used for external content already registered with the system. This is a search of local metadata and is usually a faster search than Remote Repository items.

  It is up to the adapter configuration to make adapter content visible to the Records system server. If the adapter has not made its content available, content will not be found in a search.
- **Remote Repositories Search** is used to find items stored on external content systems whether they have been cataloged on the Records system server or not. This is a search of all possible content using adapters to schedule the search. The adapters use the criteria entered for a Remote Repository Search as the criteria used for the search on that remote repository. Searching for content in Remote Repository is not in real time and is dependent on adapters to complete the search. This option provides the most accurate and up-to-date results but it may take a long time to complete.

  > **Note:**
  >
  > Federated Search adds functionality to the Search Query Builder Form. See *Using Oracle WebCenter Content* for additional help using the Search Query Builder.

- **SES Search** is similar to a Remote Repository Search but the search is not scheduled and run by an adapter. Instead, a connection is made to an SES server which has done a scheduled crawl of content on the adapter(s). Records connects directly to the SES server, which has been configured ahead of time. If this option is selected and no servers have been configured, an error message is displayed.

The Federated Query Builder page enables users to build and schedule queries across all repositories. Select the repositories to include in the search from the **External Sources** list. Multiple sources can be included in the search.

Select a field to use as sorting criteria and click **Search** when done. When performing a remote repository search, a search name must be entered. Users can only search using fields that are mapped to *all* of the selected external sources. Errors occur if a search is done against a source using a field that is not mapped.

After pressing **Save** enter a title for the action. The search is scheduled and the Federated Searches page appears. The list of scheduled searches includes the number of external sources requested in the search, and number of external sources that have completed the search request.

The search is scheduled and waits for the external search adapters to return results.

To return to the Federated Searches page, choose **Records** then **Scheduled** then **Federated Searches**.

20.2.2 Performing a Search

To perform a search of a remote repository:

1. Choose **Search** then **Global Search**.
2. Choose the type of repository search to perform.
3. On the Federated Query Builder page, select the external sources to use in the query from the pull-down list.
4. Select **Include Content** to retrieve copies of the content matching the search criteria. This option is only available when performing a remote repository search.

   Do not select this box unless search results are certain. Returning a copy of the data takes time and uses space. Fine tune the query first and verify what items will be returned before actually retrieving the content. For more information about content retrieved during a search, see About Returned Content.
5. Choose the fields to use for searching. The **Search Builder** menu is used to select fields for use in the query. Only search using fields that are mapped to *all* of the selected external sources. Errors occur if a search is done against a source using a field that is not mapped.

   After a field is selected for use, additional menus are available to further refine the criteria. Boolean operators can be used to combine fields. Click the insert symbol (a plus sign) to access a menu of Boolean operators. Click the remove symbol (a lowercase *x*) to clear previous selections. Additional wildcard search operators, such as **Matches** and **Substring**, enable further flexibility in query building.
6. Enter a search term for full-text searching. If a search is done across all sources, be aware that some adapters may not be able to perform a full text search. When choosing a search type, choose types that are valid for the adapters in use. For example, if a user chooses full-text search to use with an adapter that does not allow that option, an error is returned.
7. Enter a search name. A Federated search is performed on the adapter's schedule, so it may not occur immediately. A search name allows users to check the status of the scheduled Federated search. No uniqueness validation is performed on this field because the unique identifier is an assigned Federated Search ID.
8. Select the result output criteria by indicating a number of results per page and the sorting criteria used for the results.
9. Click **Search** when done.

   The query is routed to the chosen adapters and is completed according to the adapter configuration.

20.2.2.1 About Returned Content

Saved content is stored in a zip file and is checked into the Records system as internal content. These returned content items can be accessed and treated as standard local items. Users can set dispositions on the files, establish specific rules for their handling, and so on.

Some adapters may return the content in multiple files because the adapter may be configured to chunk data into manageable units. This behavior is controlled on the adapter side and cannot be modified.

20.2.2.2 Checking Search Progress

Federated searches are performed according to adapter schedules which may vary according to the different configurations. To check the progress of the search, choose **Records** then **Scheduled** then **Federated Searches**. Or click the Federated Searches Link on the Federated Query Builder page.

The Federated Searches List page opens. This page shows the scheduled searches and their progress. The following options are available on the **Actions** menu for each search:

- **Show Search Results:** Opens the Federated Search Results page for the selected search. If multiple external sources were selected in the search, the Search Results page organizes the results by external source. The search results for individual external sources can also be displayed.
- **Show Search Details:** Opens the details for the selected search. Within the Federated Search Details page, users can view the search results for individual external sources, freeze the search results, download the files returned for the search, and create a similar search.

> **Note:**
>
> Users can freeze items in the returned search results per external source. If multiple external sources have been defined in the search, but have not all returned results, users can schedule a freeze on the sources that returned results for the scheduled search.

- **Subscribe to Search**: Subscribes the user to the search and opens the Content Information page for the query. For more details, see Subscribing to a Search.
- **Create Similar Search:** Opens the Federated Query Builder page, pre-populated with search criteria used in the selected search. Users can modify or add criteria to schedule a new search.
- **Delete Search:** Deletes the selected scheduled search. See Deleting a Search for details.

20.2.2.3 Subscribing to a Search

When a Federated search is created, a content item is checked into the local repository with details of the search. If a user chooses **Subscribe to Search** on the

Actions menu for an item on the Federated Searches List page, the user is subscribed to the content item for that query.

As results are returned for the saved search, the content item is updated. For example, if a query is set to use three repositories and results are returned from one, the content item is updated and a notification is triggered to those people who are subscribed to the content item.

20.2.2.4 Deleting a Search

A Federated search can be deleted at any time. Search results do not have to be returned to delete the search.

To delete a search, deselect the check box for the search on the Federated Searches List page then choose **Delete** on the Table menu. A message is displayed, indicating the search and all returned results will be deleted. Any pending search results will be ignored.

20.3 Federated Freeze

Federated Freeze is used in conjunction with Federated search, to freeze search results from a Federated query.

> **Note:**
>
> Federated Freeze adds functionality to content freezing used in the Records system. See Managing Freezes for additional information about freezes.

When freezing content on an external repository, first schedule a Federated Search, then run a Federated Freeze on the returned results. If the search result that is selected for freezing has not been registered with the Records system yet, an external record is created for it automatically using the metadata returned in the search results. This new external record is then frozen.

The Frozen Federated Search Content page opens for review or further action. The list of frozen scheduled searches includes the external source of the frozen content, and the status (scheduled, completed or errors) of the freeze.

The following options are available from the **Actions** menu for a frozen item:

- **Show Freeze Errors**: Displays the items with errors during the selected freeze. Freeze errors may occur if the checked-in items from the Federated Search do not have all required fields defined or if the items do not pass validation.
- **Refreeze Errors**: Reschedules the freeze for the error items in the selected search task.
- **Delete Freeze**: Deletes the selected freeze.

This section discusses the following topics:

- Freezing Search Results
- Viewing Scheduled Freezes

20.3.1 Freezing Search Results

To freeze search results:

1. Choose **Records** then **Scheduled** then **Federated Searches**.
2. On the Federated Searches List page, choose **Show Search Results** from the **Actions** menu of a search.
3. On the Federated Search Results page, select the check box of the items to freeze then choose **Freeze** from the Table menu.
4. If freezes have been added to a My Favorites list, they appear on the list in the resulting dialog box. Choose a freeze name from the list or select **Show All Freezes** to display all defined freezes.
5. Enter a reason for the freeze.
6. Click **OK**.

   The search results are frozen.

20.3.2 Viewing Scheduled Freezes

To view which results are frozen:

1. Choose **Records** then **Scheduled**.
2. Choose **Federated Search Freezes**.

   The Frozen Federated Search Content page opens, showing all items found during a federated search that are frozen.

Part V
Managing Content Conversion

This part of the documentation discusses Oracle WebCenter Content document conversion options.

Managing Content Conversion contains the following chapters:

- Configuring Inbound Refinery
- Managing Inbound Refinery
- Working with Conversions
- Working With Image and Video Conversions
- Managing PDF Watermark
- Supported File Formats

21
Configuring Inbound Refinery

Oracle WebCenter Content: Inbound Refinery offers a variety of content conversion options depending on what components are installed and enabled on Oracle WebCenter Content Server and Inbound Refinery. This chapter provides an overview of the different conversion options and instructions on configuring Inbound Refinery.
This chapter discusses the following topics:

21.1 Prerequisites for Configuring Inbound Refinery

At minimum, the following components must be installed and enabled for basic conversion functionality.

Component Name	Component Description	Enabled on Server
InboundRefinery	Enables Inbound Refinery	Inbound Refinery Server
InboundRefinerySupport	Enables the Content Server to work with Inbound Refinery	Content Server

21.2 Content Server and Refinery Configuration Scenarios

Oracle WebCenter Content: Inbound Refinery can be used to refine content managed by Content Server. The Inbound Refinery application can be installed on the same computer as Content Server or on one or more separate computers. You must add the refinery as a provider to Content Servers on the same or separate computers after installation. For details, see Configuring Refinery Providers.

> **Note:**
>
> Inbound Refinery does not support running in a cluster environment. Inbound Refinery can do conversion work for a Content Server cluster, but cannot run in a cluster environment itself. To ensure that Inbound Refinery functions properly, Inbound Refinery creates and maintains a long-term lock on the `/queue/conversion` directory. If Inbound Refinery is mistakenly configured as part of a cluster and a second Inbound Refinery attempts to start and lock the same directory, the second Inbound Refinery will fail to start, and the attempt is logged.

Various configurations are possible, so keep the following general rules in mind when setting up a refinery environment:

- If processing a large number of content items per day, do not run Inbound Refinery on the same computer as Content Server.
- The more dedicated refinery systems that are installed, the faster the content is processed. Having more refinery systems than Content Server instances provides optimal speed. Having fewer refinery systems than Content Server instances can slow down performance when converting large numbers of files.
- Typically, there is no reason to have multiple refineries on the same computer because refineries share the system's resources. One refinery can serve as a provider to multiple Content Servers. This includes third-party applications used during conversion. To improve performance, use separate computers for each refinery.
- Some file types and large files are processed slower than average. If a large number of these types must be processed in addition to other file types, consider setting up a refinery on a separate system to process just these file types. This requires more than one refinery system, but it does provide optimum refining speed and performance.

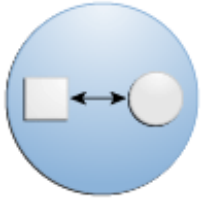
The following scenarios are common. Other refinery configurations are possible in addition to the ones described in this section. Specific content management applications might require their own particular refinery setup, which does not necessarily match any scenario mentioned in this section.

- Scenario A: One Content Server and one refinery on the same computer.
- Scenario B: Multiple Content Servers and one refinery on the same computer.
- Scenario C: Multiple Content Servers and one refinery on separate computers.
- Scenario D: One refinery per Content Server on separate computers.
- Scenario E: Multiple refineries per Content Server on separate computers.

Each of these scenarios is explained in more detail in their descriptions, including the benefits of a scenario and considerations to take into account for a scenario. In the scenario images, the following symbols are used to represent a computer, the Content Server, and the Inbound Refinery:

- Large Circle: computer
- Small Circle: Inbound Refinery
- Small Square: Content Server

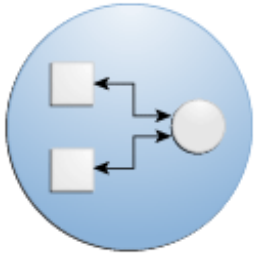
21.2.1 Scenario A



This is the most basic scenario possible. It comprises one Content Server and one refinery on the same computer.

- Benefits:
  - Least expensive and easiest to configure.
  - Only one copy of third-party applications required for refinery conversions must be purchased.
- Considerations:
  - Number and speed of conversions is limited.
  - Not as powerful as scenarios where refineries are not deployed on the Content Server computer, because refinery processing on the Content Server computer can slow searches and access to the website, and vice versa. Each conversion can take between seconds and minutes, depending on the file type and size.

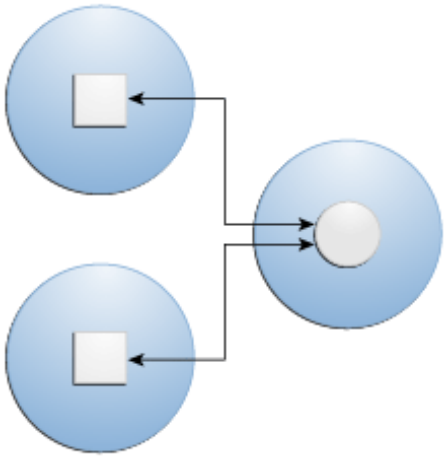
21.2.2 Scenario B



This scenario comprises multiple Content Servers and one refinery on the same computer.

- Benefits: Only one copy of third-party applications required for refinery conversions must be purchased.
- Considerations:
  - Number and speed of conversions is limited.
  - Not as powerful as scenarios where refineries are not deployed on the Content Server computer, because refinery processing on the Content Server computer can slow searches and access to the website, and vice versa. Each conversion can take between seconds and minutes, depending on the file type and size.
  - In this configuration, typically the refinery is set as a provider to one of the Content Servers. After deployment, the refinery will need to be added as a provider to the other Content Servers. For details, see Configuring Refinery Providers.

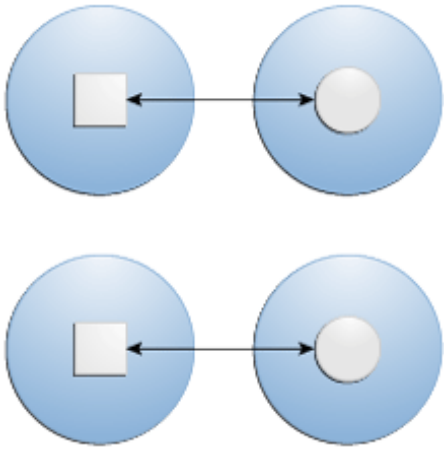
21.2.3 Scenario C



This scenario comprises multiple Content Servers and one refinery on separate computers.

- Benefits:
  - Only one copy of third-party applications required for refinery conversions must be purchased.
  - Faster processing than when the refinery is deployed on the same computer as a Content Server.
  - Refinery processing does not affect Content Server searches and access to the website, and vice versa.
- Considerations:
  - Not as powerful as scenarios where there is at least one refinery per Content Server.
  - In this configuration, typically the refinery will need to be added as a provider to each Content Server. For details, see Configuring Refinery Providers.

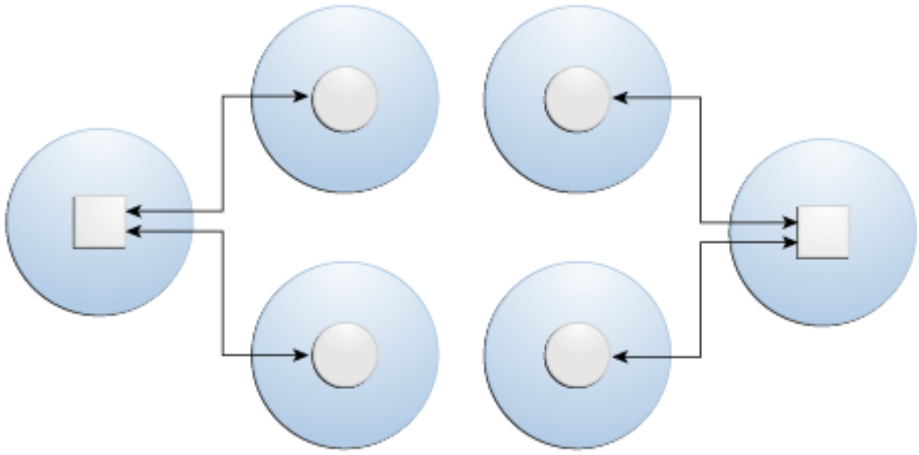
21.2.4 Scenario D



This scenario comprises one refinery per Content Server on separate computers.

- Benefits:
  - Faster processing for high volumes of content and big file sizes.
  - Refinery processing does not affect Content Server searches and access to the website, and vice versa.
- Considerations:
  - Each refinery computer needs a copy of all third-party applications required for conversion.
  - Each refinery will need to be added as a provider to each Content Server. For details, see Configuring Refinery Providers.

21.2.5 Scenario E



This scenario comprises multiple refineries per Content Server on separate computers.

- Benefits:
  - Fastest processing for high volumes of content and big file sizes.
  - Refinery processing does not affect Content Server searches and access to the website, and vice versa.
- Considerations:
  - Each refinery computer needs a copy of all third-party applications required for conversion.
  - In this configuration, typically each refinery will need to be added as a provider to each Content Server instance. For details, see Configuring Refinery Providers.

21.3 Configuring Content Server and Refinery Communication

This section discusses the following topics:

- Configuring Refinery Providers
- Editing the Refinery IP Security Filter
- Setting Library Path for UNIX Platforms

21.3.1 Configuring Refinery Providers

A Content Server communicates with a refinery through a provider. A refinery can serve as a provider for one or multiple Content Server instances. For more information about common configurations, see Content Server and Refinery Configuration Scenarios.

The refinery can be added as a provider to a Content Server instance on the same computer or added to Content Server instances on separate computers after deployment.

This section discusses the following topics:

- Adding or Editing Refinery Providers
- Disabling/Enabling Refinery Providers
- Deleting Refinery Providers

21.3.1.1 Adding or Editing Refinery Providers

To add a refinery as a provider to a Content Server instance:

1. Log into the Content Server as an administrator.
2. From the main menu, choose **Administration** then **Providers**.
3. In the **Create a New Provider** section of the Providers page, click **Add** in the Action column for the *outgoing* provider type.

4. On the Add/Edit Outgoing Socket Provider page, complete the following fields:
   - **Provider Name** (required): A name for the refinery provider.
   - **Provider Description** (required): A user-friendly description for the provider.
   - **Provider Class** (required): The name of the Java class for the provider. The default is the *intradoc.provider.SocketOutgoingProvider* class.
   - **Connection Class:** Not required.
   - **Configuration Class:** Not required.
   - **Server Host Name** (required): The host name of the server on which the refinery is installed.
   - **HTTP Server Address:** The HTTP server address for the refinery. Not required when the refinery is on the same computer as the Content Server.
   - **Server Port** (required): The port on which the refinery provider will communicate. This entry must match the server socket port configured on the post installation configuration page during deployment of Inbound Refinery. For information on post configuration, see *Installing and Configuring Oracle WebCenter Content*. The default refinery port is 5555.
   - **Instance Name** (required): The instance name of the refinery. For example, *ref2*.
   - **Relative Web Root** (required): The relative web root of the refinery is `/ibr/`.
5. Select the **Use Connection Password** check box if the refinery you are connecting to imposes authentication for the Content Server (the Content Server will share the refinery's user base). If enabled, you must specify a user name and password to be used and have the ProxyConnections component installed and configured on the refinery.
6. Select the **Handles Inbound Refinery Conversion Jobs** check box. This is required.
7. Deselect the **Inbound Refinery Read Only Mode** check box. Select this check box only when you do not want the Content Server to send new conversion jobs to the refinery.
8. If necessary, change the maximum number of jobs allowed in the Content Server's pre-converted queue. The default is 1000 jobs.
9. Click **Add**.

   The Providers page opens with the new refinery provider added to the Providers table.
10. Restart the Content Server.

To edit information for an existing refinery provider, access the Providers page and click **Info** in the Action column for the provider to edit. Make the required changes on the Add/Edit Outgoing Socket Provider page. When done, restart the Content Server instance.

21.3.1.2 Disabling/Enabling Refinery Providers

To disable or enable an existing refinery provider:

1. Log into the Content Server as an administrator.
2. From the main menu, choose **Administration** then **Providers**.
3. In the Providers table on the Providers page, click **Info** in the Action column for the refinery provider to disable or enable.
4. On the Provider Information page, click **Disable** or **Enable**.
5. Restart the Content Server.

21.3.1.3 Deleting Refinery Providers

To delete an existing refinery provider:

1. Log into the Content Server as an administrator.
2. From the main menu, choose **Administration** then **Providers**.
3. In the Providers table on the Providers page, click **Info** in the Action column for the refinery provider to delete.
4. On the Provider Information page, click **Delete**.

   A confirmation message appears.
5. Click **OK**.

21.3.2 Editing the Refinery IP Security Filter

An IP security filter is used to restrict access to a refinery. Only hosts with IP or IPv6 addresses matching the specified criteria are granted access. By default, the IP security filter is 127.0.0.1|0:0:0:0:0:0:0:1, which means the Inbound Refinery will only listen to communication from *localhost*. To ensure that a Content Server can communicate with all of its refineries, the IP or IPv6 address of each Content Server computer should be added to the refinery's IP security filter. This is true even if the refinery is running on the same computer as the Content Server instance. To edit an IP security filter for a refinery:

1. Access the refinery computer.
2. Start the System Properties application:
   - **Windows:** choose **Start** then **Programs**. Select **Oracle Content Server/ Inbound Refinery**, the *instance_name*, then **Utilities** and **System Properties**
   - **UNIX:** run the `SystemProperties` script, which is located in the /bin subdirectory of the refinery installation directory
3. Select the **Server** tab.
4. The IP Address Filter field must include the IP or IPv6 address of each Content Server computer (even if this is the same physical computer that is also running the refinery server). The default value of this field is 127.0.0.1|0:0:0:0:0:0:0:1 (localhost), but you can add any number of valid IP or IPv6 addresses. You can specify multiple IP addresses separated by the pipe symbol (|), and you can use wildcards (* for zero or many characters, and ? for single characters). For example:

   ```
   127.0.0.1|0:0:0:0:0:0:0:1|10.10.1.10|62.43.163.*|62.43.161.12?
   ```

   > **Note:**
   >
   > Always include the localhost IP address (127.0.0.1).
5. Click **OK** when you are done, and restart the refinery server.

> **Tip:**
>
> Alternately, you can add IP addresses to the IP security filter directly in the `config.cfg` file located in the *`IntradocDir`*`/config` directory. Add the IP or IPv6 address to the `SocketHostAddressSecurityFilter` variable. For example:
> `SocketHostAddressSecurityFilter=127.0.0.1|0:0:0:0:0:0:0:1|10.10.1.10|62.43.163.*`
>
> Make sure that you specify the localhost IP or IPv6 address in the `SocketHostAddressSecurityFilter` variable in the config.cfg file.

21.3.3 Setting Library Path for UNIX Platforms

Content Server and Inbound Refinery use Outside In Technology. Ouside In Technology is dynamically linked with the GCC libraries (libgcc_s and libstdc++) on all Linux platforms as well as both Solaris platforms and HPUX ia64. Content Server must be able to access these libraries, however, Solaris and HPUX do not initially make these libraries available. If running Content Server or Inbound Refinery on either Solaris or HPUX, you need to obtain and install the GCC libraries and configure Content Server to find them. For information about configuring the library paths, see Setting Library Paths in Environment Variables on UNIX Platforms in *Installing and Configuring Oracle WebCenter Content*.

21.4 Configuring Content Servers to Send Jobs to Refineries

File extensions, file formats, and conversions are used in Content Server to define how content items should be processed by Inbound Refinery and its conversion add-ons. In addition, application developers can create custom conversions.

This section discusses the following topics:

- Understanding File Formats and Conversions
- Managing File Types
- Configuring the Content Server for PassThru Files
- Configuring the Content Server Refinery Conversion Options
- Configuring Image Files to Bypass Preview
- Overriding Conversions at Check-In
- Modifying Default Content Conversion Settings

21.4.1 Understanding File Formats and Conversions

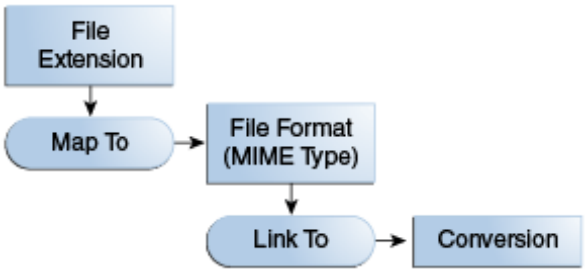
File formats are generally identified by their Multipurpose Internet Mail Extension (MIME) type, and each file format is linked to a specific conversion. Each file extension is mapped to a specific file format. Therefore, based on a checked-in file's extension, the Content Server can control if and how the file is processed by refineries. The conversion settings of the refineries specify which conversions the refineries accept and control the output of the conversions.

Consider the following example: the `doc` file extension is mapped to the file format `application/msword`, which is linked to the conversion `Word`. This means that the Content

Server attempts to send all Microsoft Word files (with the `doc` file extension) checked into the Content Server to a refinery for conversion.

As another example, if the `xls` file extension is mapped to the file format `application/vnd.ms-excel`, which is linked to the conversion `PassThru`, Microsoft Excel files are not sent to a refinery. Instead, the Content Server can be configured to place either a copy of the native file or an HCST file that points to the native vault file in the `/weblayout` directory. This means that users must have an application capable of opening the native file installed on their computer to view the file.

Figure 21-1 Mapping File Formats to a Conversion



When a file is checked into the Content Server and its file format is mapped to a conversion, the Content Server checks to see if it has any refinery providers that accept that conversion and are available to take a conversion job. This means that:

- Refinery providers must be set up for the Content Server. For details, see Configuring Refinery Providers.
- The refinery (or refineries) need to be configured to accept the conversion. For details, see Setting Accepted Conversions.

Conversions specify how a file format should be processed, including the conversion steps that should be completed and the conversion engine that should be used. For details, see Managing File Types.

Conversions available in the Content Server should match those available in the refinery. When a file format is mapped to a conversion in the Content Server, files of that format are sent for conversion upon check-in. One or more refineries must be set up to accept that conversion. For details, see Setting Accepted Conversions.

The following default conversions are available. Additional conversions might be available when conversion add-ons are installed. For more information, see the documentation for each specific conversion add-on.

Conversion	Description
PassThru	Used to prevent files from being converted. When this conversion is linked to a file format, all file extensions mapped to that file format are not sent for conversion. The Content Server can be configured to place either a copy of the native file or an HCST file that points to the native vault file in the `/weblayout` directory. For details, see Configuring the Content Server for PassThru Files.

Conversion	Description
Word	Used to send Microsoft Word, Microsoft Write, and rich text format (RTF) files for conversion. The files are converted according to the conversion settings for the refinery.
Excel	Used to send Microsoft Excel files for conversion. The files are converted according to the conversion settings for the refinery.
PowerPoint	Used to send Microsoft PowerPoint files for conversion. The files are converted according to the conversion settings for the refinery.
MSProject	Used to send Microsoft Project files for conversion. The files are converted according to the conversion settings for the refinery.
Distiller	Used to send PostScript files for conversion. The files are converted to PDF using the specified PostScript distiller engine.
MSPub	Used to send Microsoft Publisher files for conversion. The files are converted according to the conversion settings for the refinery.
FrameMaker	Used to send Adobe FrameMaker files for conversion. The files are converted according to the conversion settings for the refinery.
Visio	Used to send Microsoft Visio files for conversion. The files are converted according to the conversion settings for the refinery.
WordPerfect	Used to send Corel WordPerfect files for conversion. The files are converted according to the conversion settings for the refinery.
PhotoShop	Used to send Adobe Photoshop files for conversion. The files are converted according to the conversion settings for the refinery.
InDesign	Used to send Adobe InDesign, Adobe PageMaker, and QuarkXPress files for conversion. The files are converted according to the conversion settings for the refinery.
MSSnapshot	Used to send Microsoft Snapshot files for conversion. The files are converted according to the conversion settings for the refinery.
PDF Refinement	Used to send checked-in PDF files for refinement. Depending on the conversion settings for the refinery, this includes optimizing the PDF files for fast web viewing using the specified PostScript distiller engine.
Ichitaro	Used to send Ichitaro files for conversion. The files are converted according to the conversion settings for the refinery.
ImageThumbnail	Used to send select graphics formats for creation of simple thumbnails only. This is useful if Inbound Refinery is not installed but thumbnail images of graphics formats are wanted. The returned web-viewable files are a copy of the native file and optionally a thumbnail image. When Inbound Refinery is installed, it can be used instead of the ImageThumbnail conversion to send graphics formats for conversion, including the creation of image renditions and thumbnails.
NativeThumbnail	Used to send select file formats for creation of thumbnails from the native format rather than from an intermediate PDF conversion. Typically, this conversion is used to create thumbnails of text files (TXT), Microsoft Outlook email files (EML and MSG), and Office documents without first converting to PDF. The returned web-viewable files are a copy of the native file and optionally a thumbnail rendition and/or a an XML rendition. For an XML rendition to be created, XMLConverter must be installed and XML step configured and enabled.

Conversion	Description
MultipageTiff	Used to send files for conversion directly to multi-page TIFF files using Outside In Image Export. When file formats are mapped to this conversion, the conversion settings for the refinery are ignored, and the files are sent directly to Image Export for conversion to a TIFF file.
OutsideIn Technology	Uses Outside In X to print supported formats to PostScript for conversion with WinNativeConverter on the refinery server.
Direct PDFExport	Used to send files for conversion directly to PDF using Outside In PDF Export.
FlexionXML	Used to send files for conversion using XML Converter.
SearchML	Used to send files for conversion using XML Converter
XSLT Transformation	Used to send files for XSLT transformation using XML Converter. XSL transformation is used to output XML data into another format.
Digital Media Graphics	When Digital Asset Manager is installed, this is used to send digital images for conversion into multiple image renditions using Image Manager.
Digital Media Video	When Digital Asset Manager is installed, this is used to send digital videos for conversion into multiple video or audio renditions using Video Manager.
TIFFConversion	Used to send TIFF files for conversion to a PDF format that enables indexing of text in the document.
Word HTML	Used to send Microsoft Word files for conversion to HTML using the native Microsoft Word application.
PowerPoint HTML	Used to send Microsoft PowerPoint files for conversion to HTML using the native Microsoft PowerPoint application.
Excel HTML	Used to send Microsoft Excel files for conversion to HTML using the native Microsoft Excel application.
Visio HTML	Used to send Microsoft Visio files for conversion to HTML using the native Microsoft Visio application.

21.4.1.1 Passing Content Items Through the Refinery and Failed Conversions

When a file format is linked to the conversion `PassThru`, all file extensions mapped to that file format are not converted. When a content item with a file extension mapped to `PassThru` is checked into the Content Server, the file is not sent to a refinery, and web-viewable files are not created. The Content Server can be configured to place either a copy of the native file or an HCST file that points to the native file in the `weblayout` directory. This means that the application that was used to create the file, or an application capable of opening the file, is required on each client for the user to be able to view the file. For details, see Configuring the Content Server for PassThru Files.

If a file is sent to the refinery and the refinery notifies the Content Server that the conversion has failed, the Content Server can be configured to place a copy of the native file in the `weblayout` directory. In this case users must also have an application capable of opening the native file installed on their computer to view the file. For details, see Configuring the Content Server Refinery Conversion Options.

21.4.1.2 About MIME Types

It is recommended that you name new file formats by the MIME (Multipurpose Internet Mail Extensions) type corresponding to the file extension (for example, the format mapped to the `doc` file extension would be `application/msword`).

When a content item is checked in to Content Server, the content item's format is assigned according to the format mapped to the file extension of the native file. If the native file is not converted, Content Server includes this format when delivering the content item to clients. Using the MIME type for the format assists the client in determining what type of data the file is, what helper applications should be used, and so on.

If the native file is converted, Inbound Refinery assigns the appropriate format to the web-viewable file (for example, if a refinery generates a PDF file, it would identify this file as `application/pdf`), and Content Server then includes this format when delivering the web-viewable file to clients (instead of the format specified for the native file).

Inbound Refinery includes an extensive list of file formats configured out of the box when installed. Check the listing in the Configuration Manager applet of the Content Server provider. New formats should only need to be added if working with rare or proprietary formats.

The are several good resources on the Internet for identifying the correct MIME type for a file format. For example:

- `http://filext.com/`

21.4.2 Managing File Types

You can manage file types and file format configuration details using the File Formats Wizard page or the Configuration Manager. The File Formats Wizard page can be used to configure conversions for most common file types, however it does not replicate all of the Configuration Manager applet features.

> **Note:**
>
> The InboundRefinerySupport component must be installed and enabled on the Content Server and at least one Inbound Refinery provider enabled to enable the File Formats Wizard page. Also, conversion option components might add file types to the File Formats Wizard page.

To use the File Formats Wizard page:

1. Log in as an administrator.
2. From the main menu, choose **Administration** then **Refinery Administration** then **File Formats Wizard**.
3. On the File Formats Wizard page, select the check box for each file type to be sent to a refinery for conversion. To select or deselect all check boxes, select or deselect the check box in the heading row.
4. Click **Reset** if you want to revert to the last saved settings.
5. Click **Update**.

The corresponding default file extensions, file formats, and conversions are mapped automatically for the selected file types.

To use the Configuration Manager:

1. Log in as an administrator.
2. From the main menu, choose **Administration** then **Admin Applets**.
3. Choose **Configuration Manager**.
4. Select **Options** then **File Formats**.

21.4.2.1 Adding or Editing File Formats

To add a file format and link it to a conversion:

1. On the File Formats page, in the File Formats section, click **Add**.
2. On the Add New/Edit File Formats page, in the Format field, enter the name of the file format. Any name can be used, but Oracle recommends that you use the MIME type associated with the corresponding file extension(s).
3. From the Conversion list, choose the appropriate conversion.
4. In the Description field, enter a description for the file format.
5. Click **OK** to save the settings.

To edit a file format, select the file format and click **Edit**. On the Add New/Edit File Formats page, make the appropriate changes.

21.4.2.2 Adding or Editing File Extensions

To add a file extension and map it to a file format (and thus associate the file extension with a conversion):

1. On the File Formats page, in the File Extensions section, click **Add**.
2. On the Add/Edit File Extensions page, in the Extension field, enter the file extension.
3. From the **Map to Format** list, choose the appropriate file format from the list of defined file formats. Selecting a file format directly assigns all files with the specified extension to the specific conversion that is linked to the file format.
4. Click **OK** to save the settings.

To edit a file extension, select the file extension on the File Formats page and click **Edit**. Make the appropriate changes.

21.4.3 Configuring the Content Server for PassThru Files

When a file format is linked to the conversion `PassThru`, all file extensions mapped to that file format are not sent for conversion. By default, the Content Server places a copy of the native file in the `weblayout` directory. However, the Content Server can be configured to place an HCST file that points to the native vault file in the `weblayout` directory instead. This can be useful if you have large files that are not being converted, and you do not want to copy the large files to the `weblayout` directory.

Please note the following important considerations:

- The contents of the HCST file are controlled by the contents of the `redirectionfile_template.htm` file.
- The `GET_FILE` service is used to deliver the file, so no PDF highlighting or byte serving is available. This can be resolved by overriding the template and reconfiguring the web server.
- A simple template is used; the browser's **Back** button might not be functional and layout differences might occur. This can be resolved by overriding the template and reconfiguring the web server.
- There is no reduction in the number of files because there is still an HCST file in the `weblayout` directory. However, there can be disk space savings if the native vault file is large.
- This setting has no affect on files that are sent to a refinery for conversion; that is, if a file is sent to a refinery for conversion, another Content Server setting controls whether web-viewable files or a copy of the native file are placed in the `weblayout` directory, and an HCST file cannot be used. For more information, see Configuring the Content Server Refinery Conversion Options.

To configure the Content Server to place an HCST file in the `weblayout` directory instead of a copy of the native file:

1. Using a text editor, open the Content Server `config.cfg` file located in the *`IntradocDir`*`/config/` directory.
2. Include the `IndexVaultFile` variable, and set the value to `true`:

   ```
   IndexVaultFile=true
   ```

3. Save your changes to the `config.cfg` file.
4. Restart the Content Server.

21.4.4 Configuring the Content Server Refinery Conversion Options

You can configure how a Content Server interacts with its refinery providers, including how the Content Server should handle pre and post-converted jobs.

> **Note:**
>
> The InboundRefinerySupport component must be installed and enabled on the Content Server and at least one Inbound Refinery provider enabled to make the Inbound Refinery Conversion Options page available.

To configure how the Content Server should handle pre- and post-converted jobs:

1. Log into the Content Server as an administrator.
2. From the main menu, choose **Administration** then **Refinery Administration** then **Conversion Options**.
3. On the Refinery Conversion Options page, enter the following information:
   - Enter the number of seconds between successive transfer attempts for preconverted jobs. The default is 10 (seconds).

- Enter the native file compression threshold size in MB. The default threshold size is 1024 MB (1 GB). Unless the native file exceeds the threshold size, it is compressed before the Content Server transfers it to a refinery. This setting is used to avoid the overhead of compressing very large files (for example, large video files). If you do not want any native files to be compressed before transfer, set the native file compression threshold size to 0.
- If you want the conversion to fail when the time for transferring a job expires, select the check box.
- Determine how you want the Content Server to handle failed conversions. If a file is sent to a refinery and conversion fails, the Content Server can be configured to place a copy of the native file in the `/weblayout` directory ("Refinery Passthru"). To enable `Passthru`, select the check box. To disable `Passthru`, deselect the check box.

  Please note the following important considerations:

  – When a file is sent to the refinery for conversion, an HCST file cannot be used instead of a copy of the native file. For more information on configuring how the Content Server handles files that are not sent to the refinery, see Configuring the Content Server for PassThru Files.

  – This setting can also be overridden manually using the `AllowPassthru` variable in the `config.cgf` file located in the *`IntradocDir`*`\config\` directory.

4. Click **Reset** if you want to revert to the last saved settings or click **Update** to save the changes.
5. Restart the Content Server.

21.4.5 Configuring Image Files to Bypass Preview

For common image file formats, the native user interface typically displays a preview of the native document that most web browsers can display. In contrast, the Oracle WebCenter Content user interface typically uses Outside In technology to convert native documents into page images before displaying a preview of the document on the View Documents page.

For multilayer image files, such as animated `.gif` files, Outside In creates one image for every layer of the multilayer file. This results in a separate page for every layer in the original image. Because most web browsers can correctly display animated `.gif` files and other multilayer formats, you may want Content Server to bypass Outside In so that the animation displays correctly.

To bypass Outside In and instead display the native file, an administrator lists the formats in the `SimplePreviewFormatList` variable in the content server `intradoc.cfg` file. This should be done for formats supported by browsers accessing the content server, such as standard image formats. This allows the browser to display the native file and correctly interpret the multiple layers of animated file formats.

To specify what image formats you want to use a simple preview:

1. Use a text editor to open the `intradoc.cfg` file located in the Content Server *`DomainDir`*`/ucm/cs/bin` directory.
2. Specify the image formats to use a simple preview in a comma separated list. For example:

```
SimplePreviewFormatList=image/gif,image/png
```

3. Save your changes to the `intradoc.cfg` file.
4. Restart the content server.

21.4.6 Overriding Conversions at Check-In

Certain file extensions might be used in multiple ways in your environment. A good example is the ZIP file extension. For example, you might be checking in:

- Multiple TIFF files compressed into a single ZIP file that you want a refinery with Tiff Converter to convert to a single PDF file with OCR.
- Multiple file types compressed into a single ZIP file that you do not want sent to a refinery for conversion (the ZIP file should be passed through in its native format).

When using a file extension in multiple ways, the Content Server can be configured to enable the user to choose how a file is converted when they check the file into the Content Server. This is referred to as *Allow override format on checkin*. To enable this Content Server functionality:

1. Log in as an administrator.
2. From the main menu, choose **Administration** then **Admin Server** then **General Configuration**.
3. Enable the **Allow override format on checkin** check box.
4. Click **Save**.
5. Using the Configuration Manager, map the file extension to the conversion that is used most commonly to make it the default conversion. For example, for the ZIP file extension, you might set up the following default conversion:
   - Map the ZIP file extension to the `application/zip` file format, and the `application/zip` file format to the `TIFFConversion` conversion. Thus, by default it would be assumed that ZIP files contain multiple tiff files and should be sent to a refinery with Tiff Converter for conversion to PDF with OCR.
6. Using the Configuration Manager, set up the alternate file formats and conversions that you want to be available for selection by the user at check-in. Continuing the preceding example for the ZIP file extension, you might set up the following alternate conversions:
   - Map the `application/zip-passthru` file format to the `PassThru` conversion. This option could then be selected at check-in for a ZIP file containing a variety of files that should not be sent to a refinery for conversion. The ZIP file would then be passed through in its native format.
7. Restart the Content Server.

   When a user checks in a file, the user can override the default conversion by selecting any of the conversions you have set up.

Enabling users to override conversions at check-in is often used in conjunction with multiple dedicated refineries and custom conversions. Continuing the preceding example for the ZIP file extension, you might have one refinery set up with Tiff Converter, which would be used to convert ZIP files containing multiple tiff files to PDF with OCR, and a second refinery set up to convert ZIP files containing Microsoft Office files to PDF.

21.4.6.1 Changing the Size of Thumbnails

By default, thumbnails are displayed as 100 x 100 pixels. To display at a different size:

1. Open the `config.cfg` file located in the *`IntradocDir`*`/config/` directory in a text editor.
2. Change the following variables as needed to change the thumbnail height and width:
   - `ThumbnailHeight=xxx` (where `xxx` is the value in pixels)
   - `ThumbnailWidth=xxx` (where `xxx` is the value in pixels)

   Scaling is done based on whichever setting is smaller (the height setting is used if the settings are equal), preserving the aspect ratio.
3. Save the changes.
4. Restart the Content Server.

> **Note:**
>
> This updates the size of all of your thumbnails.

For more information about the `ThumbnailHeight` and `ThumbnailWidth` variables, see ThumbnailHeight and ThumbnailWidth in *Configuration Reference for Oracle WebCenter Content*.

21.4.7 Modifying Default Content Conversion Settings

After content items are checked in and before they are sent to the refinery, Dynamic Converter executes the `pre_submit_to_conversion` include resource. This include resource acts as a placeholder for any custom component that you create. The custom component overrides the value of the `dConversion` variable for the content item which specifies the action taken by the refinery.

To modify the default conversion criteria, you can create a custom component to modify the `pre_submit_to_conversion` resource. For example, you can selectively include or exclude full-text indexing for content items based on their MIME types or based on the value of any metadata field, including custom metadata fields.

The custom component you create loads after the default include and effectively replaces the content with the content you provide. For information about creating custom components, see *Developing with Oracle WebCenter Content*.

- Conversion Resource
- Settings for the dConversion Variable
- Conversion Resource Include Example

21.4.7.1 Conversion Resource

The default script for the `pre_submit_to_conversion` include contains sample code enclosed as a comment. The sample code does not execute, but is provided as one example of how you could modify the `dConversion` variable:

```
[[%
 The pre_submit_to_conversion include can be used to reset a
 document conversion type based on specified metadata field values.
 Create a custom component to override the sample content in this
 include.   The sample include below is enclosed as a comment and does
 not execute.
%]]
<@dynamichtml pre_submit_to_conversion@>
[[%
<$if strEquals(dDocTitle, "skip Conversion")$>
  <$dConversion="PassThru"$>
<$elseif strEquals(dDocType, "Image")$>
  <$dConversion="MultipageTiff"$>
<$endif$>
%]]
<@end@>
```

In the sample code, if the title of the content item (the value of the `dDocTitle` metadata field) is `"Skip Conversion"`, then the content item is not converted (`dConversion` is given the value of `"PASSTHRU"`). Also by default, if the document type (the value of the `dDocType` metadata field) is `"Image"`, then the content item is converted to a multi-page TIFF image file.

21.4.7.2 Settings for the dConversion Variable

The value of the `dConversion` variable determines how a checked-in content item is converted. The format for the `dConversion` variable is:

```
dConversion="<conversion_type>"
```

21.4.7.3 Conversion Resource Include Example

Scenario:

When a user checks in Word document, they can choose to either convert the document as a Word document or to pass the document through unconverted.

Solution:

To allow users to determine whether a Word document are converted or not, you can create a custom metadata field (for example, `xPerformConversion`) with a list that has two values: `Yes` and `No` with `No` as the default. When a user checks in a Word document that is to be converted, they set the value of `xPerformConversion` field to `Yes` during check in.

To implement this solution, create a custom component whose content is as follows:

```
<@dynamichtml pre_submit_to_conversion@>
<$if strEquals(xPerformConversion, "No")$>
   <$dConversion="PASSTHRU"$>
<$elseif strEquals(xPerformConversion, "Yes")$>
   <$dConversion="Word"$>
```

```
<$endif$>
<@end@>
```

21.5 Viewing Status Details

This section discusses how to view the status of conversion jobs. The following topics are discussed:

- Viewing Refinery Conversion Status
- Viewing IBR Provider Status

21.5.1 Viewing Refinery Conversion Status

To view refinery conversion status, use the main menu to choose **Administration** then **Refinery Administration** then **Conversion Options**. You can also click the **Conversion Job Status** tab on the IBR Provider Status page.

> **Note:**
>
> The InboundRefinerySupport component must be installed and enabled and at least one Inbound Refinery provider enabled for this page to be available.

The following conversion status information is available.

Element	Description
Refresh	Updates the status of the displayed jobs.
Force Job Queue Check	Forces Content Server to deliver jobs to refinery providers. This is particularly useful if a refinery has gone down, causing any pending jobs to fail. In this situation, pending jobs are periodically resubmitted to providers for conversion. This button forces the submission.
Conversion Job ID	A unique identifier assigned by Inbound Refinery to each submitted job.
Content ID	The unique Content Server identifier of the content item submitted for conversion.
Conversion Job State	Identifies where a job is in the conversion process.
Job Submitted to Provider	Identifies the provider to which a job is submitted.
Last Action At	Lists the date and time of the last change in job state.
Actions	Links to the Content Server content information page of the content item submitted for conversion.

21.5.2 Viewing IBR Provider Status

To view IBR Provider status, use the main menu to choose **Administration** then **Refinery Administration** then **IBR Provider Status**. You can also click the **IBR Provider Status** tab on the Refinery Conversion Job Status page.

> **Note:**
>
> The InboundRefinerySupport component must be installed and enabled on the Content Server and at least one Inbound Refinery provider enabled for this page to be available.

The following conversion information appears on the IBR Provider Status page.

Element	Description
Force Status Update	Refreshes the status of the displayed providers.
Provider	The name of each provider.
Available	Identifies whether a provider is accepting content for conversion.
Read Only	Identifies if a provider is read only, meaning that it can no longer accept jobs for conversion. It can only return conversions to Content Server.
Jobs Queued	Identifies the number of jobs each provider has waiting for conversion.
Last Message	Displays the last status message delivered by the provider.
Connection State	Identifies whether the provider is connected to the Content Server or not.
Last Activity Date	Lists the date and time of the last provider activity.
Actions	Displays the Provider Information page, listing information regarding the specific provider.

21.6 Configuring Refinery Conversion Settings

Before configuring refinery conversion settings, you should complete the following tasks:

- Start your refinery.
- Verify that your refinery has been set up as a provider to one or multiple Content Servers. For details, see Configuring Refinery Providers.
- Verify that the InboundRefinerySupport component is installed and enabled on each Content Server.
- Verify that each Content Server has been configured to send files to the refinery for conversion. For details, see Configuring Content Servers to Send Jobs to Refineries.

Refinery conversion settings control which conversions the refinery will accept and how the refinery processes each conversion. Inbound Refinery includes Outside In Image Export, which can be used for the following.

- Create thumbnails of files. Thumbnails are small preview images of content. For details, see Setting Up Thumbnails.
- Convert files to multi-page TIFF files, enabling users to view the files through standard web browsers with a TIFF viewer plugin. For details, see S.

In addition, several conversion options are available for use with Inbound Refinery. When a conversion option is enabled, its conversion settings are added to the refinery.

This section discusses the following topics:

21.6.1 Calculating Timeouts

As content is processed by a refinery, it is allotted a certain amount of processing time based on the size of the file and the settings on the Timeout Settings page. The timeout value, in minutes, is calculated as follows:

timeout value [in minutes] =([file size in bytes] x timeout factor) /60,000

In order to determine what file to use, Inbound Refinery first checks if the previous step produced a file. If so, that file is used in the timeout calculations. Otherwise, the native file is used. If the previous step output more than one file (for example, Excel to PostScript), the sum of the file sizes is used. The content item to be processed is allotted at least the number of minutes indicated in the Minimum column, but no more minutes than indicated in the Maximum column. If the calculated timeout value is lower than the minimum value, the minimum value applies. If the calculated timeout value is larger than the maximum value, the maximum value applies.

21.6.1.1 Timeout Calculations

The following examples show how timeouts are calculated:

- **Example 1**

  File size =10 MB (10485760 bytes or 10240 KB)
  Minimum =2
  Maximum =10
  Factor =3

  Calculated Timeout =10485760 *3 /60000 =524.288 minutes =8.74 hours

In this case, Inbound Refinery will wait only the maximum of 10 minutes.

- **Example 2**

  File size =200 KB (204800 bytes)
  Minimum =2
  Maximum =30
  Factor =2

  Calculated Timeout =204800 *2 /60000 =6.83 minutes

In this case, Inbound Refinery will wait only the calculated 6.83 minutes and not the Maximum of 30 minutes.

- **Example 3**

  File size =50 KB (51200 bytes)
  Minimum =2
  Maximum =30
  Factor =2

  Calculated Timeout =51200 *2 /60000 =1.71 minutes

  In this case, Inbound Refinery will wait the minimum of 2 minutes and not the calculated timeout or the Maximum of 30 minutes

21.6.2 Setting Accepted Conversions

To set the conversions that the refinery will accept and queue maximums:

1. Log into the refinery.
2. Choose **Settings** then **Conversions**.
3. On the Conversion Listing page, set the total number of conversion jobs that are allowed to be queued by the refinery. The default is 0 (unlimited).
4. Enter the maximum number of conversions allowed to wait for pick up by a Content Server before Inbound Refinery will no longer accept conversion jobs from that Content Server. The default is 1000.
5. Enter the number of seconds that the refinery should be considered busy when the maximum number of conversions has been reached. The default is 120 (seconds). When the maximum number of conversion jobs for the refinery has been reached, Content Servers will wait this amount of time before attempting to communicate with the refinery again.
6. Enter the maximum number of conversions that the refinery should process at the same time. The default is 5.
7. Select the check box for each conversion that you want the refinery to accept.
   - By default, all conversions are selected and accepted.
   - To select all conversions, select the **Accept** check box in the column heading.
   - To deselect all conversions, deselect the **Accept** check box in the column heading.
8. Set the maximum number of jobs (across all refinery queues) for each conversion type. The default is 0 (unlimited).
9. Click **Update** to save your changes.
10. Restart each Content Server that is an agent to the refinery to effect your changes in the Content Server's queuing immediately. Otherwise, the changes in refinery's accepted conversions will not be known to the Content Server until the next time it polls the refinery.

21.6.3 Setting Multi-Page TIFF Files as the Primary Web-Viewable Rendition

Inbound Refinery includes Outside In Image Export, used to convert files to multi-page TIFF files as the primary web-viewable rendition. This enables users to view the files through standard web browsers with a TIFF viewer plugin.

Other conversion options, such as PDF Export, are used to create other types of renditions as the primary web-viewable rendition. When conversion options that can generate a web-viewable rendition are enabled, additional options for the options are available.

To set multi-page TIFF files as the primary web-viewable rendition that the refinery will generate:

1. Log into the refinery.
2. Choose **Settings** then **Conversions**.
3. On the Conversions page, select **Convert to Multipage TIFF image** to convert files to multipage TIFF files as the primary web-viewable rendition.
4. Click **Update** to save the changes.

21.6.4 Setting Up Thumbnails

Thumbnails are small preview images of content used on search results pages and typically link to the web-viewable file they represent. A thumbnail provides consumers with a visual sample of a file without actually opening the file itself. This enables them to check a file before committing to downloading the larger, original file.

Inbound Refinery includes Outside In Image Export, which can be used to create thumbnails of files. Please note the following important considerations:

- You must configure the file formats and conversions in each Content Server to send files to the refinery for thumbnailing. For details, see Configuring Content Servers to Send Jobs to Refineries. The refinery must be configured to accept the conversions. For details, see Setting Accepted Conversions.
- The Outside In Image Export thumbnail engine cannot successfully create thumbnails of PDF files with Type 3 Fonts. If a checked in PDF file contains Type 3 Fonts, the Outside In Image Export thumbnail engine will create a thumbnail with a blank page.
- Thumbnail files are stored as JPEG, GIF, or PNG files in Content Server's the weblayout directory with the characters *@t* in their filenames. For example, the file *Report2001@t~2.jpg* is the thumbnail that belongs to *Report2001~2.pdf* (which is revision 2 of a file called *Report2001.xxx*).
- Thumbnails cannot be processed for any files that are encrypted or are password-protected.
- Thumbnails can be created for EML files. If you are using Internet Explorer and have installed the April, 2003, Cumulative Patch for Outlook Express, you will receive an error if you click on the thumbnail to view an EML file. This only applies if the primary web-viewable file is an EML file (a multi-page TIFF or a PDF version of the EML file was not generated by the refinery as the primary web-viewable file,

and the native EML file was copied to the `weblayout` directory as the primary web-viewable file).

- Thumbnails of EML files do not exactly match the look-and-feel of the EML file as opened in Outlook Express because the thumbnail is created based on a plain-text rendition, whereas Outlook Express opens the file in its own format.
- For details about changing the size of thumbnails displayed in the Content Server, see Changing the Size of Thumbnails.
- Note that if thumbnails are turned off in Inbound Refinery, any thumbnails already created are still displayed on the search results pages.

Thumbnails are the only additional rendition available in Inbound Refinery by default. Other conversion options and custom conversions enable you to create additional renditions.

To enable thumbnails and configure thumbnail settings:

1. Log into the refinery.
2. Choose **Settings** then **Conversions**.
3. On the Conversions page, in the Additional Renditions Options column, select **Create Thumbnail Rendition**.
4. Click **Update** to save your changes.
5. Click **Settings**, then **Options**.
6. Under Thumbnail Options, click **Configure**.
7. In the Thumbnail Options page, select the necessary thumbnail options. Click **Update** when done.

> **Note:**
>
> When using Inbound Refinery on a SPARC system running Solaris, or any system running Linux, by default Outside In Image Export uses its internal graphics code to render fonts and graphics. You can also choose to use the operating system's native graphics subsystem instead. For details, see Configuring Rendering Options on UNIX.

The following table describes the available options.

Element	Description
Create Thumbnail Image from the Native Vault File check box	Specifies whether the thumbnail image is created from the native file or the primary web-viewable file.
Page Number of Native Vault File to Use to Create Thumbnail Image field	Specifies which page of the native file is used to create the thumbnail image. The default setting is 1. The first page of the native file is used to create the thumbnail image.
Use quick sizing radio button	Specifies the fastest conversion of color graphics but the quality of the converted graphic is somewhat degraded.
Use smooth sizing radio button	Specifies a more accurate representation of the original graphic, but requires a more complex process which slows down the conversion speed slightly. This is the default setting.
Smooth sizing for grayscale graphics radio button	Use the smooth sizing option for grayscale graphics and the quick sizing option for any color graphics.

Element	Description
Produce jpg thumbnails radio button	Specifies that all thumbnails be created as JPG files. This is the default thumbnail file type setting.
Produce gif thumbnails radio button	Specifies that all thumbnails be created as GIF files.
Produce png thumbnails radio button	Specifies that all thumbnails be created as PNG files.
Update button	Saves changes to settings.
Reset button	Reverts to the last saved settings.

21.6.5 Configuring Rendering Options on UNIX

When running Inbound Refinery on Linux or Solaris SPARC systems and creating multi-page TIFF files or thumbnails, by default Outside In uses its internal graphics code to render fonts and graphics. Therefore, access to a running X Window System display server (X Server) and the presence of either Motif (Solaris) or LessTif (Linux) is not required. The system only needs to be able to locate usable fonts. Fonts are not provided with Outside In. For information about setting the path to usable fonts, see Specifying the Font Path.

To configure Inbound Refinery so that Image Export uses the operating system's native graphics subsystem to render fonts and graphics instead of its internal graphics code:

1. Log in to the Inbound Refinery computer as the Inbound Refinery user.

   The Inbound Refinery computer must have access to a running X Window System display server (X Server) and the presence of either Motif (Solaris) or LessTif (Linux).

2. Ensure that the `DISPLAY` variable in the Inbound Refinery startup script (`.profile`, `.login`, `.bashrc`, and so on) points to the running X Server. For example:

   ```
   DISPLAY=:0.0
   export DISPLAY
   ```

3. Source the new `.profile` (for example, using `/usr/bin/sh`, run the command:

   ```
   ..profile
   ```

4. Give Outside In Image Export permission to use the running X Server with the following command:

   ```
   xhost +localhost
   ```

5. Lock the console, leaving the Inbound Refinery user logged in.
6. Log into the refinery.
7. Choose **Settings** then **Options**.
8. On the Options page, click **Configure** under the General OutsideIn Filter Options section.
9. Select **Use native operating system's native graphics subsystem**.
10. Click **Update**.

21.6.6 Specifying the Font Path

For Inbound Refinery to work properly, you must specify the path to fonts used to generate font images. By default, the font path is set to the font directory in the JVM used by Inbound Refinery: *java.home*/lib/fonts. However, the fonts included in the default directory are limited and may cause poor renditions. Also, in some cases if a non-standard JVM is used, then the JVM font path may be different than that specified as the default. If this is the case, an error message is displayed from both Inbound Refinery and Content Server. If this error occurs, ensure the font path is set to the directory containing the fonts necessary to properly render your conversions.

To configure Inbound Refinery to locate usable fonts:

1. Log in to the Inbound Refinery computer as the Inbound Refinery user.
2. Under **Administration**, select **Admin Server**, then **General Configuration**.
3. Enter the path to the font directories to be used by Outside In in the text field. For example, on Linux:

   ```
   /usr/lib/X11/fonts/TTF
   ```

   For example, on Windows:

   ```
   C:\WINDOWS\Fonts
   ```

   If fonts are called for and cannot be found, Outside In will exit with an error. Only TrueType fonts (**.ttf* or **.ttc* files) are supported.
4. Click **Save**.

21.6.7 Configuring Timeout Settings for Graphics Conversions

To configure timeout settings for graphics conversions:

1. Log into the refinery.
2. Choose **Settings** then **Timeouts**.
3. On the Timeouts page, enter the **Minimum (in minutes)**, **Maximum (in minutes)**, and **Factor** for graphics conversions. For details, see Calculating Timeouts.
4. Click **Update** to save the changes.

22

Managing Inbound Refinery

This chapter discusses the administrative information and tasks needed to manage Oracle WebCenter Content: Inbound Refinery, such as user authentication, single sign-on, managing agents and providers, configuring web server filters, and publishing dynamic and static layout files.
This chapter discusses the following topics:

22.1 Managing Refinery Authentication and Users

As a managed server running within an Oracle WebLogic Server domain, user and group access to Inbound Refinery is controlled by Oracle WebLogic Server and system security configuration is handled through the WebLogic Server console.

If additional services are required, such as Oracle Internet Directory or single sign-on using Oracle Access Manager, these can be linked to the Oracle WebLogic Server domain managing Inbound Refinery using WebLogic Server controls.

When deployed, the *refineryadmin* Inbound Refinery role has permissions to administer Oracle Inbound Refinery. Any user needing administration rights to Inbound Refinery must be part of the corresponding *refineryadmin* group in Oracle WebLogic Server.

For additional information, see the following documentation.

Table 22-1 Additional System Security Documentation

Task	Where to Go For More Information
Administering Oracle WebLogic Server	*Administering Oracle Fusion Middleware*
Administering Oracle WebCenter Content	*Administering Oracle WebCenter Content*

22.2 Managing Refinery Conversion Queues

A refinery is set up as a provider to a Content Server instance. When a file is checked into the Content Server, a copy of the native file is stored in the `/vault` directory (the native file repository). The native file is the format in which the file was originally created (for example, Microsoft Word).

If the file format is set up to be converted, the Content Server creates a conversion job in its pre-converted queue. The Content Server then attempts to deliver the conversion job to one of its active refinery providers (a refinery that is configured to accept the conversion and is not busy). The Content Server sends the conversion parameters to an active refinery.

When the refinery receives conversion parameters, it returns the following data to the Content Server:

- **JobAcceptStatus:** The status can be one of the following.

Status	Description	Content Server Action
ERROR	There was an unexpected error in processing the request.	The content item is left in GenWWW status and removed from the Content Server's pre-converted queue.
NEVER_ACCEPT	The refinery is not configured to accept the conversion, and it will never accept the job.	The refinery provider is marked as unavailable until the conversion job is cleared from the pre-converted queue
ACCEPT	The refinery will take the conversion job.	The job is removed from the pre-converted queue, transferred to the refinery, and expected to be converted.
BUSY	The refinery could take the conversion job, but it has reached its total queue maximum or the maximum number of conversion jobs for a specific conversion.	The refinery provider is not used again until the RefineryBusyTimeSeconds it provides to the Content Server has elapsed.

- **JobAcceptStatusMsg**: A string that explains the refinery's status, to be logged by both the refinery and the Content Server.
- **JobCanAccept**: A boolean that indicates if the job was accepted.
- **RefineryBusyTimeSeconds**: The number of seconds the refinery wants to be left alone (this is just a hint; the refinery will not stop accepting requests).

If the refinery does not accept the job, the Content Server tries the next available refinery. The Content Server keeps attempting to transfer the job until a refinery accepts the job or the maximum transfer time is reached. If the maximum transfer time is reached, the job is removed from the Content Server's pre-converted queue and the content item remains in GenWWW status.

When a refinery accepts the job, the Content Server then uploads a ZIP file, containing the conversion data and the file to be converted, to the refinery. The Content Server also places an entry in its RefineryJobs table, which it uses to track the conversion job. The refinery places the conversion job in its pre-converted queue.

The refinery then attempts to perform the specified conversion, calling the appropriate conversion options as necessary. When the refinery finishes processing the conversion job, it places it in its post-converted queue. The Content Server polls the refinery periodically to see if conversion jobs in its RefineryJobs table have been completed. When the refinery reports that it has finished processing a conversion job, the Content Server downloads any converted files (for example, a web-viewable thumbnail file and a PDF file) from the refinery, places the conversion job in its post-converted queue, and kicks off any post-conversion functionality as needed.

Refinery queue management settings can be configured both on the Content Server and on the refinery. The following pages are used to manage refinery queues:

- Refinery Conversion Options page: This page contains settings that affect how the Content Server interacts with all of its refinery providers.
  - **Seconds between successive transfer attempts:** Used to set the number of seconds between successive transfer attempts for each conversion job. By default, the Content Server waits 10 seconds between attempts to deliver a conversion job to one of its refinery providers.
  - **Minutes allowed to transfer a single job:** Used to set the number of minutes allowed for the transfer of each conversion job. By default, the Content Server attempts to transfer a conversion job to one of its refinery providers for 30 minutes.
  - **Native file compression threshold**: Used to set the native file compression threshold size in MB (default size is 1024 MB (1 GB)). Unless the native file exceeds the threshold size, it is compressed before the Content Server transfers it to a refinery. This setting avoids the overhead of compressing very large files, such as video files. To leave native files uncompressed before transfer, set the threshold size to 0.
  - **When the time for transferring a job expires, the conversion should fail**: Used to specify the time to failure for a conversion. When the maximum allowed time for transferring a conversion job is reached, the conversion job is removed from the Content Server's pre-converted queue and the content item remains in GenWWW status. If specified that the conversion job should fail, the content item remains in GenWWW status. A conversion error is displayed on the Content Information page with a **Resubmit** button, allowing the user to resubmit the content item for conversion.
  - **When a conversion sent to an Inbound Refinery fails, set the conversion to 'Refinery Passthru':** Used to specify how the Content Server handles failed conversions. If a file is sent to a refinery and conversion fails, the Content Server can be configured to place a copy of the native file in the weblayout directory by enabling refinery passthru.

    > **Note:**
    >
    > When a file is sent to the refinery for conversion, an HCST file cannot be used instead of a copy of the native file. For more information on configuring how the Content Server handles files that are not sent to the refinery, see Configuring the Content Server for PassThru Files.

- Add/Edit Outgoing Socket Provider page: Used to specify settings for an individual refinery provider.

  - **Handles Inbound Refinery Conversion Jobs:** Used to specify if the provider handles conversion jobs. If this option is not selected, the Content Server does not attempt to transfer any conversion jobs to or from the provider.
  - **Inbound Refinery Read Only Mode:** Used to prevent the Content Server from sending new conversion jobs to the refinery provider. However, the refinery provider continues to return conversion jobs as the jobs are finished.

The following refinery pages contain information and settings used to manage refinery queues:

- Items in Queue page: Used to view items in the pre and post-converted queues for a specific refinery agent (such as a Content Server).
- Conversion Listing page: Used to view items in the pre and post-converted queues for a specific refinery agent (such as a Content Server).
  - **Maximum number of conversions allowed to be queued**: Used to set the total number of conversion jobs allowed to be queued by the refinery. Default: 0 (unlimited).
  - **Maximum number of conversions in post conversion queue**: Used to specify the number of conversions allowed to be queued in the post conversion queue of a refinery. Default: 1000.
  - **Number of seconds the refinery should be considered busy**: Used to specify the number of seconds the refinery is considered busy when the maximum number of conversions is reached. Default: 30 (seconds). When the maximum number of conversion jobs for the refinery is reached, Content Servers wait this amount of time before attempting to communicate with the refinery again.
  - **Maximum conversions**: You can specify the maximum number of jobs the refinery can process at the same time. The default is 5.

22.3 Managing Refinery Agents

The following tasks are performed when managing agents:

- Verbose Logging
- Deleting Agents

22.3.1 Verbose Logging

You can enable verbose logging for each refinery agent. When verbose logging is on, general agent status information, a detailed description of each conversion engine action (for example, when the conversion was started and file details, conversion step details, and conversion results), and errors are recorded in the refinery agent log. When verbose logging is off, only general agent status information and errors are recorded in the refinery agent log.

To enable verbose logging for a refinery agent:

1. Log in to the refinery.
2. Select **Refinery Administration** then **Agent Management**.
3. On the Agent Management page, select the **Enable Verbose Logging** check box for the refinery agent.

4. To revert to the last saved settings, click **Reset**.
5. Click **Update** to save your changes.

22.3.2 Deleting Agents

A refinery agent can be deleted only when there are no conversion jobs in the refinery agent's pre or post-converted queues. To delete a refinery agent:

1. Log in to the refinery.
2. Select **Refinery Administration** then **Agent Management**.
3. On the Agent Management page, select **Delete Agent** from the Actions menu for the refinery agent.
4. On the Delete Agent page, select the **Confirm deletion of agent *agent_name*** check box to confirm that you want the agent deleted. History, logs, and any jobs in the agent queue are also deleted.
5. Click **Delete Agent**.

22.4 Managing Refinery Providers

You should not need to configure any refinery providers. To view refinery provider information using the web-based Inbound Refinery interface:

1. Log in to the refinery.
2. From the navigation menu, choose **Refinery Administration** then **Providers**.

22.5 Viewing Refinery Information

This section discusses methods to view refinery information:

- Viewing Refinery Configuration Information
- Viewing Refinery System Audit Information

22.5.1 Viewing Refinery Configuration Information

To view the configuration information for the refinery using the web-based Inbound Refinery interface:

1. Log in to the refinery.
2. From the navigation menu, choose **Refinery Administration** then **Configuration Information**.

   The Configuration Information page opens, showing an overview of the main system settings. In addition, it lists all installed server components or custom components that are currently enabled and disabled.

The Configuration Information page is for information purposes only and cannot be edited.

22.5.2 Viewing Refinery System Audit Information

To view the system audit information for the refinery using the web-based Inbound Refinery interface:

1. Log in to the refinery.
2. From the navigation menu, choose **Refinery Administration** then **System Audit Information**.

   The System Audit Information page opens, showing information which may be useful while troubleshooting a problem or adjusting a server's performance. The General Information section of this page provides the following information:

   - Information regarding whether the system is receiving too many requests.
   - Information about the memory cache for the system, which is useful in troubleshooting any "out of memory" errors you may receive. This is important when running the refinery server with many users and a large quantity of data.
   - Information about which Java threads are currently running. This is useful in determining the cause of an error.
   - Listing of any audit messages.

   Tracing in a refinery can be activated on a section-by-section basis. Tracing for active sections is displayed on the Console Output page. Section tracing is useful for determining which section of the server is causing trouble, or when you want to view the details of specific sections. Sections can be added by appending extra sections to create a comma separated list.

   A listing of the sections available for tracing, with brief descriptions, is available by clicking the information icon next to the Tracing Sections Information heading. For example, activating *refinery* displays extended information about conversion status, activating *ref-config* traces changes to the current running environment, and activating *refsteplogic* traces the logic that determines what conversion steps are used. The wildcard character *is supported so that *ref** will trace all sections that begin with the prefix *ref*, including *refinery*, *ref-config*, and *refsteplogic*.

   Some tracing sections also support verbose output. Enable **Full Verbose Tracing** if you wish to see in-depth tracing for any active section that supports it.

> **Note:**
>
> Any options set on this page are lost when the refinery is restarted unless you enable **Save** and click **Update**.

22.6 Configuring the Web Server Filter

To configure the web server filter for a refinery using the web-based Inbound Refinery interface:

1. Log in to the refinery.
2. From the navigation menu, chose **Refinery Administration** then **Filter Administration**.

   The Configure Web Server Filter page opens. This page is used to configure and troubleshoot the web server filter communication with the refinery.

22.7 Publishing Dynamic and Static Layout Files

To publish dynamic and static layout files:

1. Log in to the refinery.
2. To publish your dynamic layout files, choose **Administration** then **Admin Actions**, and under the Weblayout Publishing section select **publish dynamic layout files**. The PUBLISH_WEBLAYOUT_FILES service is executed.

   All dynamic refinery layout files (`.css` files and `.js` files) are published from the refinery *`IntradocDir`*`/shared/config/templates` directory to the `weblayout` directory. This service is used when customizing the refinery. The PUBLISH_WEBLAYOUT_FILES service is also executed each time the refinery is restarted.
3. To publish static layout files, choose **Administration** then **Admin Actions**, and under the Weblayout Publishing section select **publish static layout files**. The PUBLISH_STATIC_FILES service is executed.

   All static layout files (graphic files) are published from the refinery *`IntradocDir`*`/shared/publish` directory to the `weblayout` directory. This service is used when customizing your refinery. The PUBLISH_STATIC_FILES service is not executed each time your refinery is restarted, as it can be very time-consuming to execute. This service must be executed manually when customizing the refinery.

For more information about other publishing options available and for customizing the content and refinery servers, see the documentation provided with Content Server.

22.8 Active Virus Scanning on Windows

When running Inbound Refinery on Windows, active virus scanning of some Inbound Refinery and Content Server directories can cause conversions to fail.

Exclude the following Content Server directories from active virus scanning:

- the `weblayout` directory (*`WeblayoutDir`*)
- the `vault` directory (*`VaultDir`*)
- *`IntradocDir`*`\data\`
- *`IntradocDir`*`\search\`

> **Tip:**
>
> The Content Server `\vault\~temp` directory should not be excluded, as it is the most important directory to scan.

Exclude the following Inbound Refinery directories from active virus scanning:

- the `vault` directory (*`VaultDir`*)
- the `weblayout` directory (*`WeblayoutDir`*)
- *`IntradocDir`*`\data\`

> **Tip:**
>
> If these directories must be scanned, it is recommended that physical disk scanning be used on the Content Server and Inbound Refinery computers during off-peak hours rather than actively scanning these directories. For best results, a local anti-virus program should be used to scan local drives.

22.9 Changing the Date Format and Time Zones

This section discusses changing the default date format and the default time zone setting:

- Changing the Date Format
- Setting the Time Zone

22.9.1 Changing the Date Format

The default English-US locale uses two digits to represent the year ('yy'), where the year is interpreted to be between 1969 and 2068. For example, 65 is considered to be 2065, not 1965. If you want years prior to 1969 to be interpreted correctly in the English-US locale, you must change the default date format for that locale to use four digits to represent years ('yyyy').

This issue does not apply to the English-UK locale, which already uses four digits for the year.

To modify the default English-US date format:

1. Start the System Properties utility:
   - **Microsoft Windows:** Select **Start** then **Programs** then **Oracle Content Server**. Choose ***refinery_instance*** then **Utilities** then **System Properties**.
   - **UNIX:** Start the `SystemProperties` script, which is located in the `/bin` subdirectory of the refinery's installation directory.
2. Select the **Localization** tab.
3. Select the English-US entry in the list of locales, and click **Edit**.
4. On the Configure Locale dialog, modify the date format to use four digits for the year ('yyyy') rather than two ('yy').
5. After you are done editing, click **OK** to close the Configure Locale dialog.
6. Click **OK** to apply the change and exit System Properties.
7. Stop and restart the refinery.

22.9.2 Setting the Time Zone

During the installation of Inbound Refinery, you might have indicated that you wanted to use the default time zone for the selected system locale. If that is the case, the installer attempted to automatically detect the time zone of the operating system and set the refinery time zone accordingly. In certain scenarios, the time zone of the

operating system might not be recognized. The time zone will then be set to the UTC time zone (Universal Time Coordinated), which is the same as Greenwich Mean Time (GMT).

You then need to set the time zone manually:

1. Start the System Properties utility:
   - **Microsoft Windows:** Select **Start** then **Programs** then **Oracle Content Server**. Choose ***refinery_instance*** then **Utilities** then **System Properties**.
   - **UNIX:** Start the SystemProperties script, which is located in the `/bin` subdirectory of the refinery's installation directory.
2. Select the **Server** tab.
3. From the **System Timezone** list, choose the time zone you want to use for the refinery.
4. Click **OK** to apply the change and exit System Properties.
5. Stop and restart the refinery.

22.10 Monitoring Refinery Status

Log files are created to help monitor the refinery status. Agent are entities, such as a Content Server, that sends a job to the refinery. Conversion status information is separated and logged by agent to make it easier to view the information and find details.

Two types of log files are created for the refinery:

- Refinery logs: These logs contain general information about refinery functionality that is not specific to conversions performed for agents (for example, startup information). One log file is generated for each day the refinery is running. For more information, see Viewing Refinery Status.
- Refinery Agent logs: These logs contain information specific to conversions performed for agents sending conversion jobs to the refinery. One log file is generated for each agent, each day that the agent sends at least one conversion job to the refinery. For more information, see Viewing Agent Statuses.

22.10.1 Viewing Refinery Status

Entries are added to the appropriate log file throughout the day as events occur and are listed by date and time. The time stamp placed on a refinery log entry designates when the log entry was created, not necessarily when the action took place.

Refinery agent log entries list the conversion number at the beginning of each entry because each agent can have multiple concurrent conversions running at a given time. For example: *Log entry for conversion job '3513'*. The following types of log entries are generated.

Log Entry	Description
Info	Displays status information. For example, startup information or a description of a conversion engine action.
Error	Displays errors that occur.

Verbose logging can be enabled. When on, it records general agent status information, a detailed description of each conversion engine action (for example, when the conversion was started and file details, conversion step details, and conversion results), and errors. When

verbose logging is off, only general agent status information and errors are recorded in the refinery agent log.

A log file might include **Details** links. Clicking the **Details** links expands and collapses log details. Typically, the log details are either a stack dump or a trace back to the code that generated the error.

The following sections describe how to view different types of conversion status information:

- Viewing Conversion Statuses
- Viewing Refinery Logs
- Viewing Console Output
- Viewing Conversion History

22.10.1.1 Viewing Conversion Statuses

The refinery creates each agent when it sends its first conversion job to the refinery. Until then, information for the agent is not available in the refinery.

To view the current status of conversions for all refinery agents:

1. Log in to the refinery.
2. Choose **Home** from the main menu, or choose **Status** then **Refinery Status** from the Main menu.

22.10.1.2 Viewing Refinery Logs

To view the refinery log files:

1. Log in to the refinery.
2. Choose **Home** in the main menu and select the **Refinery Logs** tab, or choose **Status** then **Refinery Status** from the Main menu and select the **Refinery Logs** tab.
3. On the Refinery Logs page, click a log link to display the refinery log.

22.10.1.3 Viewing Console Output

To view the refinery console output:

1. Log in to the refinery.
2. Choose **Home** from the Main menu and select the **Console Output** tab, or choose **Status** then **Refinery Status** from the Main menu and select the **Console Output** tab.
   - Click **Update** to refresh the console output.
   - Click **Clear** to clear the console output.

22.10.1.4 Viewing Conversion History

To view the last fifty conversions in the conversion history for a specific refinery agent:

1. Log in to the refinery.

2. Choose **Status** then ***agent_name*** from the menu and select the **Conversion History** tab, or choose **View Conversion History** from the Actions menu for the agent on the Refinery Status page.
3. On the Conversion History page, click a Content ID link to display the Conversion Detail page.

22.10.2 Viewing Agent Statuses

The status of a specific agent can be viewed as well as the queues for all agents.

- Viewing Specific Status
- Viewing Agent Queues
- Viewing Agent Logs

22.10.2.1 Viewing Specific Status

To view the current status of conversions for a specific refinery agent:

1. Log in to the refinery.
2. Navigate to the Agent Status page in one of the following ways:
   - Click the agent name.
   - Select **Status** then ***agent_name*** from the navigation menu.
   - Select **View Detailed Status** from the Actions menu for the agent on the Refinery Status page.

22.10.2.2 Viewing Agent Queues

To view the items that are in the pre and post-converted queues for a specific refinery agent:

1. Log in to the refinery.
2. From the navigation menu, choose **Status** then ***agent_name*** and select the **Items in Queue** tab, or choose **View Items In Queue** from the **Actions** menu for the agent on the Refinery Status page.
3. On the Items in Queue page, click **Refresh** to update the information on the page.

22.10.2.3 Viewing Agent Logs

To view the log files for a specific refinery agent:

1. Log in to the refinery.
2. From the navigation menu, choose **Status** then ***agent_name*** and choose the **Agent Logs** tab, or choose **View Agent Logs** from the Actions menu for the agent on the Refinery Status page.
3. On the Agent Logs page, click a log link to display the refinery agent log.

23
Working with Conversions

When using Oracle WebCenter Content: Inbound Refinery, several different conversion operations can be configured and managed including PDF conversion, XML conversion, Tiff conversion, and converting Microsoft Office files to HTML. This chapter discusses the tasks involved in managing those conversion types.

> **Note:**
>
> Native conversions fail when Inbound Refinery is run as a service on win64 platforms. This is due to the fact that services on win64 platforms do not have access to printer services. If performing native conversions, Inbound Refinery should not be run as a service.

For additional information describing the different types of conversion, how and where they are performed, and the advantages of each type, see the "Conversions in WebCenter Content" blog.

This chapter includes the following topics:

- Managing PDF Conversions
- Managing Tiff Conversions
- Managing XML Conversions
- Converting Microsoft Office Files to HTML

23.1 Managing PDF Conversions

Inbound Refinery can convert native files to PDF by either exporting to PDF directly using Oracle Outside In PDF Export (included with Inbound Refinery) or by using third-party applications to output the native file to PostScript and then using a third-party PDF distiller engine to convert the PostScript file to PDF.

PDF conversions require the following components to be installed and enabled on the Inbound Refinery server.

Component Name	Component Description	Enabled on Server
PDFExportConverter	Enables Inbound Refinery to use Oracle OutsideIn to convert native formats directly to PDF without the use of any third-party tools. PDF Export is fast, multi-platform, and allows concurrent conversions.	Inbound Refinery Server

Component Name	Component Description	Enabled on Server
WinNativeConverter	Enables Inbound Refinery to convert native files to a PostScript file with either the native application or OutsideInX and convert the PostScript file to PDF using a third-party distiller engine. This component is for Windows platform only. It replaces the functionality previously made available in the deprecated PDFConverter component. WinNativeConverter offers the best rendition quality of all PDF conversion options when used with the native application on a Windows platform. This does not allow concurrent conversions. WinNativeConverter also enables Inbound Refinery to convert native Microsoft Office files created with Word, Excel, PowerPoint and Visio to HTML using the native Office application.	Inbound Refinery Server

> **Note:**
>
> Native conversions fail when Inbound Refinery is run as a service on win64 platforms. This is due to the fact that services on win64 platforms do not have access to printer services. If performing native conversions, Inbound Refinery should not be run as a service.

This section describes how to work with PDF conversions and includes the following topics:

- PDF Conversion Considerations
- Configuring PDF Conversion Settings

23.1.1 PDF Conversion Considerations

There are several factors to consider when choosing a PDF conversion method. System performance (the time it takes to convert a file to PDF format), the fidelity of the PDF output (how closely it matches the look and formatting of the native file), what native applications are needed (such as Microsoft Word or PowerPoint, used to generate the PostScript file converted by Inbound Refinery), and the platform a conversion application requires should all be taken into consideration.

If the speed of conversion is a primary concern, using PDF Export to convert original files directly to PDF is fastest. In addition to not having to use third-party tools, PDF Export allows concurrent PDF conversions and supports Windows, Linux and UNIX platforms.

If the fidelity of the PDF output is a primary concern, then using the native application to open the original file, output to PostScript, and convert the PostScript to PDF is the best option. However, this method is limited to the Windows platform and it cannot run concurrent PDF conversions.

Table 23-1 compares conversion methods and lists the platforms they support.

> **Note:**
>
> Regardless of the conversion option used, a PDF is a web-ready version of the native format. A converted PDF should not be expected to be an exact replica of the native format. Many factors such as font substitutions, complexity and format of embedded graphics, table structure, or issues with third-party distiller engines may cause the PDF output to differ from the native format.

Table 23-1 PDF Conversion Methods

Conversion Method	Performance	Fidelity	Supported Platforms	Concurrent PDF Conversions
PDF Export	Best	Good	Windows/UNIX	Yes
3rd-Party Native Applications	Good	Best	Windows	No

23.1.2 Configuring PDF Conversion Settings

This section discusses the following topics regarding PDF conversion settings:

- Configuring Content Servers to Send Jobs to Inbound Refinery
- Setting PDF Files as the Primary Web-Viewable Rendition
- Installing a Distiller Engine and PDF Printer
- Configuring Third-Party Application Settings
- Configuring Timeout Settings for PDF Conversions
- Setting Margins When Using Outside In

23.1.2.1 Configuring Content Servers to Send Jobs to Inbound Refinery

File extensions, file formats, and conversions are used in Content Server to define how content items should be processed by Inbound Refinery and its conversion add-ons. Each Content Server must be configured to send files to refineries for conversion. When a file extension is mapped to a file format and a conversion, files of that type are sent for conversion when they are checked into the Content Server. Use either the File Formats Wizard or the Configuration Manager to set the file extension, file format, and conversion mappings.

All conversions required for Inbound Refinery are available by default in Content Server. For more information about configuring file extensions, file formats, and conversions in your Content Servers, see About MIME Types and Managing File Types.

Conversions available in the Content Server should match those available in the refinery. When a file format is mapped to a conversion in the Content Server, files of that format are sent for conversion upon check-in. One or more refineries must be set up to accept that conversion. Set the conversions that the refinery will accept and queue maximums on the Conversion Listing page. All conversions required for Inbound Refinery are available by default in both Content Server and Inbound Refinery.

For more information about setting accepted conversions, see Setting Accepted Conversions.

23.1.2.2 Setting PDF Files as the Primary Web-Viewable Rendition

To set PDF files as the primary web-viewable rendition:

1. Log into the refinery.
2. Select **Conversion Settings, then select Primary Web Rendition**.
3. On the Primary Web-Viewable Rendition page, select one or more of the following conversion methods. For a conversion method to be available, the associated components must be installed and enabled:
   - **Convert to PDF using PDF Export**: when running on either Windows or UNIX, Inbound Refinery uses Outside In PDF Export to convert files directly to PDF without the use of third-party applications. PDFExportConverter must be enabled on the refinery server.
   - **Convert to PDF using third-party applications**: when running on Windows, Inbound Refinery can use several third-party applications to create PDF files of content items. In most cases, a third-party application that can open and print the file is used to print the file to PostScript, and then the PostScript file is converted to PDF using the configured PostScript distiller engine. In some cases, Inbound Refinery can use a third-party application to convert a file directly to PDF. For this option to be available, WinNativeConverter must be enabled on the refinery server. In addition, when using this option, Inbound Refinery requires the following:
     - A PostScript distiller engine.
     - A PostScript printer.
     - The third-party applications used during the conversion.
   - **Convert to PDF using Outside In:** Inbound Refinery includes Outside In, which can be used with WinNativeConverter on Windows to create PDF files of some content items. Outside In is used to print the files to PostScript, and then the PostScript files are converted to PDF using the configured PostScript distiller engine. When using this option, Inbound Refinery requires only a PostScript distiller engine.

   Inbound Refinery attempts to convert each incoming file based on the conversion method assigned to the format by the Content Server. If the format is not supported for conversion by the first selected method, Inbound Refinery checks to see if the next selected method supports the format, and so on. Inbound Refinery will attempt to convert the file using the first selected method that supports the conversion of the format.

   For example, consider that you select both the **Convert to PDF using third-party applications** option and the **Convert to PDF using Outside In** option. You then

send a Microsoft Word file to the refinery for conversion. Because the Microsoft Word file format is supported for conversion to PDF using a third-party application (Microsoft Word), Inbound Refinery attempts to use the *Convert to PDF using third-party applications* method to convert the file to PDF as the primary web-viewable rendition.

If this method fails, Inbound Refinery does not attempt the **Convert to PDF using Outside In** method. However, if you send a JustWrite file to the refinery for conversion, this file format is not supported for conversion to PDF using the **Convert to PDF using third-party applications** method, so Inbound Refinery will check to see if this format is supported by the **Convert to PDF using Outside In** method. Because this format is supported by Outside In, Inbound Refinery will attempt to convert the file to PDF using Outside In.

4. Click **Update** to save your changes.
5. When using the Convert to PDF using Third-Party Applications method or the Convert to PDF using Outside In method, click the corresponding **PDF Web-Viewable Options** button.
6. On the PDF Options page, set your PDF options, and click **Update** to save your changes.

23.1.2.3 Installing a Distiller Engine and PDF Printer

When converting documents to PDF using WinNativeConverter, a distiller engine and PDF printer must be obtained, installed, and configured. This is not necessary when converting to PDF using Outside In PDF Export to open and save documents to PDF.

WinNativeConverter can use several third-party applications to create PDF files of content items. In most cases, a third-party application that can open and print the file is used to print the file to PostScript, and then the PostScript file is converted to PDF using the configured PostScript distiller engine. In some cases, WinNativeConverter can use a third-party application to convert a file directly to PDF.

> **Note:**
>
> A distiller engine is not provided with Inbound Refinery. You must obtain a distiller engine of your choice. The chosen distiller engine must be able to execute conversions via a command-line. The procedures in this section use AFPL Ghostscript as an example. This is a free, robust distiller engine that performs both PostScript to PDF conversion and optimization of PDF files during or after conversion.

To install the PDF printer:

1. Obtain and install a distiller engine on the computer where Inbound Refinery has been deployed.
2. Start the SystemProperties utility:
   - **Microsoft Windows:** Choose **Start** then **Programs** then **Oracle Content Server**. Choose ***refinery_instance*** then **Utilities** then **System Properties**.
3. Open the **Printer** tab.
4. Click **Browse** next to the **Printer Information File** field and navigate to the printer information file installed with your distiller engine.

5. Enter a name for the printer in the **Printer Name** field.
6. Enter the name of the printer driver in the **Printer Driver Name** field. This name should match the name used in the printer driver information file.
7. Enter the port path in the **Printer File Port Path** field. For example, `c:\temp\idcout.ps`
8. Click **Install Printer** and follow the printer install instructions when prompted.

> **Note:**
>
> After a printer is installed, the fields on the System Properties **Printer** tab are disabled. If the installed printer is deleted, the Printer tab is enabled again and the printer must be reinstalled.

9. Click **OK** to apply the change and exit System Properties.

23.1.2.4 Configuring Third-Party Application Settings

To change third-party application settings:

1. Log into the refinery.
2. Select **Conversion Settings** then **Third-Party Application Settings**.
3. On the Third-Party Application Settings page, click **Options** for the third-party application.
4. Change the third-party application options.
5. Click **Update** to save your changes.

23.1.2.5 Configuring Timeout Settings for PDF Conversions

To configure timeout settings for PDF file generation:

1. Log into the refinery.
2. Select **Conversion Settings** then **Timeout Settings**.
3. On the Timeout Settings page, enter the **Minimum (in minutes)**, **Maximum (in minutes)**, and **Factor** for the following conversion operations:
   - **Native to PostScript**: the stage in which the original (native) file is converted to a PostScript (PS) file.
   - **PostScript to PDF**: the stage in which the PS file is converted to a Portable Document Format (PDF) file.
   - **FrameMaker to PostScript**: these values apply to the conversion of Adobe FrameMaker files to PS files.
   - **PDF to Post Production**: the stage in which any processing is performed after the file has been converted to PDF format.
4. Click **Update** to save your changes.

23.1.2.6 Setting Margins When Using Outside In

Inbound Refinery includes Outside In version 8.3.2. When using Outside In to convert graphics to PDF, you can set the margins for the generated PDF from 0–4.23 inches or 0–10.76 cm. By default, Inbound Refinery uses 1-inch margins on the top, bottom, right, and left.

To adjust these margins:

1. Use a text editor to open the `intradoc.cfg` file located in the refinery *`DomainDir`*`/ucm/ibr/bin` directory.
2. Change the following settings:

```
OIXTopMargin=
OIXBottomMargin=
OIXLeftMargin=
OIXRightMargin=
```

3. To change the margin units from inches to centimeters, set the following:

```
OIXMarginUnitInch=false
```

4. Save your changes to the `intradoc.cfg` file.
5. Restart the refinery.

23.2 Managing Tiff Conversions

Tiff conversion enables the following functionality specific to TIFF (Tagged Image File Format) files:

- Creation of a managed PDF file from a single or multiple-page TIFF file.
- Creation of a managed PDF file from multiple TIFF files that have been compressed into a single ZIP file.
- OCR (Optical Character Recognition) during TIFF-to-PDF conversion. This enables indexing of the text within checked-in TIFF files, so that users can perform full-text searches of these files.

The TiffConverter component is supported on Windows only. For information on file formats and languages that can be converted by PdfCompressor, see the documentation provided by CVISION.

> **Note:**
>
> The TiffConverter component requires CVISION CVista PdfCompressor to perform TIFF-to-PDF conversion with OCR. PdfCompressor is not provided with the TiffConverter component. You must obtain PdfCompressor from CVISION.

TIFF conversions require the following components to be installed and enabled on the specified server.

Component Name	Component Description	Enabled on Server
TiffConverter	Enables Inbound Refinery to convert single or multipage TIFF files to PDF complete with searchable text.	Inbound Refinery Server
TiffConverterSupport	Enables Content Server to support TIFF to PDF conversion.	Content Server

23.2.1 Configuring Content Servers to Send Jobs for Tiff Conversion

File formats and conversion methods are used in Content Server to define how content items should be handled by Inbound Refinery and the conversion options. Installing and enabling the TiffConverterSupport component on a Content Server adds three TIFFConversion options on the File Formats Wizard page.

For a content item to be processed by Inbound Refinery, its file extension (for example, TIF or TIFF) must be mapped to a format name associated with the TIFFConversion conversion method. The added conversion options for Tiff Converter are not automatically mapped. They must be mapped manually. The following topics describe how to set the mappings:

- Using the File Formats Wizard for Tiff Conversion
- Using the Configuration Manager for Tiff Conversion
- Tips for Processing Zip Files in Tiff Conversion

23.2.1.1 Using the File Formats Wizard for Tiff Conversion

File formats and conversion methods for Inbound Refinery can be managed in Content Server using the File Formats Wizard. You can convert TIFF to PDF with OCR or TIFF to PDF without OCR.

To convert TIFF to PDF with OCR:

1. Log in to the Content Server as an administrator.
2. From the main menu, choose **Administration** then **Refinery Administration** then **File Formats Wizard**.
3. On the File Format Wizard page, select **tiff, tif** to enable **Convert TIFF to PDF (TIFFConversion)** in the **File Type (conversion name)** field menu. Selecting this menu item maps the TIF and TIFF file extensions to the image/tiff file format and associates the image/tiff file format with the TIFFConversion conversion method. When TIF or TIFF files are checked into the Content Server, they are processed by the refinery using Tiff Converter and converted to PDF with OCR. Deselecting this check box sets the image/tiff file format to PASSTHRU, so TIF and TIFF files are not processed by Inbound Refinery.

> **Note:**
>
> The TIFFConversion conversion method is only available when the TiffConverterSupport component has been installed and enabled, and the Content Server has been restarted.

4. If you have added `tifz` and `tiz` file extensions using the Configuration Manager, you can select **tifz, tiz** on the **File Format Wizard** page to enable **application/zip** options in the **File Type (conversion name)** field menu.
   - **Compressed Tiff to PDF (tifz, tiz)**: Selecting this menu item maps the TIFZ and TIZ file extensions to the graphic/tiff-x-compressed file format and associates the graphic/tiff-x-compressed file format with the TIFFConversion conversion method. When TIFZ or TIZ files are checked into the Content Server, they are processed by the refinery using Tiff Converter and converted to PDF with OCR. Deselecting this check box sets the graphic/tiff-x-compressed file format to PASSTHRU, so TIFZ and TIZ files are not processed by Inbound Refinery.
   - **Compressed Tiff to PDF (zip)**: Selecting this menu item maps the ZIP file extension to the application/zip file format and associates the application/zip file format with the TIFFConversion conversion method. When ZIP files are checked into the Content Server, they are processed by the refinery using Tiff Converter and converted to PDF with OCR. Deselecting this check box sets the application/zip file format to PASSTHRU, so that ZIP files are not processed by Inbound Refinery.
5. Click **Update** to save all changes.

To convert TIFF to PDF without OCR:

1. Log in to the Content Server as an administrator.
2. From the main menu, choose **Administration** then **Refinery Administration** then **File Formats Wizard**.
3. On the File Format Wizard page, select **tiff, tif to enable Convert TIFF to PDF (Direct PDFExport)** in the **File Type (conversion name)** field menu. Selecting this menu item maps the TIF and TIFF file extensions to the image/tiff file format and associates the image/tiff file format with the Direct PDFExport conversion method. When TIF or TIFF files are checked into the Content Server, they are processed by the refinery using oit PDFExport and converted to PDF without OCR.

> **Note:**
>
> When the **TIFF to PDF (Direct Export)** options is used, only the metadata in the resulting PDF is searchable, the text is not searchable.

4. Click **Update** to save all changes.

23.2.1.2 Using the Configuration Manager for Tiff Conversion

File formats and conversion methods for Inbound Refinery can be managed in Content Server using the Configuration Manager. To make changes:

1. Log in to Content Server as an administrator.

2. From the main menu, choose **Administration**, then **Admin Applets**.
3. From the Applets list, choose **Configuration Manager**.

   The Configuration Manager applet is started.
4. In the Configuration Manager applet, choose **Options** then **File Formats**.
5. To enable single, unzipped TIFF files (TIF and TIFF) to be processed by Inbound Refinery:
   a. In the File Formats section, check that the **image/tiff** file format is added and associated with the **TIFFConversion** conversion method.

      > **Note:**
      >
      > The TIFFConversion conversion method is only available when the TiffConverterSupport component has been installed and enabled, and the Content Server has been restarted.

   b. In the File Extensions section, check that the **tif** and **tiff** file extensions are added and mapped to the **image/tiff** file format.
6. To enable TIFF files that have been compressed into a single TIFZ or TIZ file to be processed by Inbound Refinery:
   a. In the File Formats section, check that the **graphic/tiff-x-compressed** file format is and associated with the **TIFFConversion** conversion method.
   b. In the File Extensions section, check that the **tifz** and **tiz** file extensions are added and mapped to the **graphic/tiff-x-compressed** file format.
7. To enable TIFF files that have been compressed into a single ZIP file to be processed by Inbound Refinery:
   a. In the File Formats section, check that the **application/zip** file format is added and associated with the **TIFFConversion** conversion method.
   b. In the File Extensions section, check that the **zip** file extension is added and mapped to the **application/zip** file format.

23.2.1.3 Tips for Processing Zip Files in Tiff Conversion

The ZIP file extension might be used in multiple ways in your environment. For example, you might be checking in:

- Multiple TIFF files compressed into a single ZIP file for Inbound Refinery to convert to a single PDF file with OCR.
- Multiple file types compressed into a single ZIP file that should not be processed (the ZIP file should be passed through in its native format).

When using the ZIP file extension in multiple ways, Oracle recommends configuring the Content Server to allow the user to choose how ZIP files are processed at check-in. This is referred to as **Allow override format on check-in**. To enable this Content Server functionality:

1. Log in to Content Server as an administrator.
2. From the main menu, choose **Administration**, then **Admin Server** then **General Configuration**.

3. Enable the **Allow override format on checkin** setting and click **Save**.
4. Restart the Content Server.
5. Using the Configuration Manager, set up the file formats:
   - Map the **application/zip** file format to the **TIFFConversion** conversion method. This option can then be selected to send ZIP files containing TIFF files to Inbound Refinery. For a description, enter `Zipped Tiff to PDF`.
   - Set up an alternate file format, for example called **application/zip-passthru**, mapped to **PassThru** for zipped files that should not be converted. For a description, enter `Zip Passthru`.

   > **Note:**
   >
   > The Content check-in Form page lists file formats by their description.

6. Map the **ZIP** file extension to the file format that will be used most commonly. This will be the default conversion method for ZIP files.
7. When a user checks in a ZIP file, the user can override the default conversion method by selecting any of the conversion methods that are set up.

> **Note:**
>
> If you are using the upload applet to check in multiple files, the files are compressed into a single ZIP file before being checked in. In this case Oracle also recommends enabling **Allow override format on check-in** so the user can choose how the ZIP file is processed when uploading multiple TIFFs.

> **Tip:**
>
> When CVista PdfCompressor merges multiple TIFF files from a compressed ZIP file, the input files are added in lexicographic order according to the standard ASCII character set.

23.2.2 Configuring Tiff Conversion Settings

This section discusses the following topics regarding conversion settings:

- Setting Accepted Conversions
- Changing Timeout Settings

23.2.2.1 Setting Accepted Conversions

When installed on the refinery, the TiffConverter component adds the TIFFConversion option to the Conversion Listing page. This conversion option must be enabled for the refinery to perform conversions on items submitted by the Content Server.

23.2.2.2 Changing Timeout Settings

The timeout settings should reflect the processing time required for the size of TIFF files that are commonly checked in to the Content Server. This is highly variable depending on CPU power and TIFF complexity. Perform these tasks to determine the appropriate timeout values for TIFF files:

- Run and time several representative Inbound Refinery jobs using CVista PdfCompressor alone (without the Inbound Refinery).
- Examine the document history information and evaluate the required processing time.
- Change Inbound Refinery timeout settings accordingly.

> **Note:**
>
> Information about Tiff Converter timeouts is recorded in the Inbound Refinery and agent logs.

To configure timeout settings for Tiff to PDF file generation:

1. Log into the refinery.
2. Choose **Settings** then **Timeouts**.
3. On the Timeouts page, enter the **Minimum (in minutes)**, the **Maximum (in minutes)**, and **Factor** for the **Tiff to PDF Conversion**. This is the stage in which the original (native) TIFF file is converted to a Portable Document Format (PDF) file.following conversion operations:

   For more information about how timeout settings are calculated and examples, see Configuring Inbound Refinery.
4. Click **Update** to save all changes.

23.2.3 Configuring CVista PdfCompressor

This section discusses the following topics regarding the CVista PdfCompressor:

- Changing PdfCompressor Settings
- Configuring CVista PdfCompressor OCR Languages

23.2.3.1 Changing PdfCompressor Settings

These options are specific to CVista PdfCompressor. If the TiffConverter component is not installed, the CVista PdfCompressor Options are not available.

To change the PdfCompressor settings:

1. Login to the refinery.
2. Choose **Conversion Settings** then **Third-Party Applications Settings**.
3. On the Third-Party Application Settings page, click **Options** for CVista PdfCompressor.

4. On the CVista PdfCompressor Options page, set the path to the location of the CVista PdfCompressor executable in the appropriate text box.
5. Enter the string of parameter values in the parameters option text box. A default option string is set on installation of the TiffConverter component.
6. Click **Update** to save the settings.

> **Tip:**
>
> When CVista PdfCompressor merges multiple TIFF files from a compressed ZIP file, the input files are added in lexicographic order according to the standard ASCII character set.

The following recommended parameter strings should produce optimal results for each given scenario. If these settings do not produce the intended results, modify these strings by removing or appending settings. For more information on these and other available settings, see the online help provided with CVista PdfCompressor (especially "Appendix A: Command-Line Flags for Compression").

Default CVista PdfCompressor Parameters - OCR Enabled

A default string is set when the TiffConverter component is installed unless a string already exists (if the string was set using a previous version of Tiff Converter). The default string has been optimized for typical PdfCompressor usage with OCR enabled:

```
-m -c ON -colorcomptype 2 -mrcquality 5 -mrcColorCompType 0 -linearize -o -ocrmode 1 -ot
120 -qualityc 75 -qualityg 75 -rscdwndpi 300 -rsgdwndpi 300 -rsbdwndpi 300 -cconc -ccong
```

CVista PdfCompressor Parameters- Horizontal and Vertical OCR Enabled

The following string can be used for typical usage with OCR and support OCR processing of both vertical and horizontal text in the same image (add -ocrtwod):

```
-m -c ON -colorcomptype 2 -mrcquality 5 -mrcColorCompType 0 -linearize -o -ocrmode 1 -ot
120 -ocrtwod -lsize 25 -qualityc 75 -qualityg 75 -rscdwndpi 300 -rsgdwndpi 300 -rsbdwndpi
300 -cconc -ccong
```

CVista PdfCompressor Parameters - No OCR

The following string can be used for simple conversion (without OCR):

```
-m -c ON -colorcomptype 2 -mrcquality 5 -mrcColorCompType 0 -linearize -qualityc 75 -
qualityg 75 -rscdwndpi 300 -rsgdwndpi 300 -rsbdwndpi 300 -cconc -ccong
```

23.2.3.2 Configuring CVista PdfCompressor OCR Languages

> **Note:**
>
> Changes made in the CVista PdfCompressor user interface do not affect how CVista PdfCompressor functions when called by Tiff Converter.

By default, CVista PdfCompressor uses an English OCR dictionary when performing OCR on TIFF files. However, CVista PdfCompressor can perform OCR on several other languages.

To set up multiple OCR languages and enable the user to choose the OCR language at check-in:

> **Note:**
>
> If the following method is used, language parameters should not be specified or passed to the refinery via the CVista PdfCompressor Options Page.

1. Obtain the appropriate current language files by contacting CVISION:
   - A `lng` file is required for each language.
   - Czech, Polish, and Hungarian also require the `latin2.shp` file.
   - Russian also requires the `cyrillic.shp` file.
   - Greek also requires the `greek.shp` file.
   - Turkish also requires the `turkish.shp` file.
2. Place the CVISION language files in the CVista installation directory. The default location is `C:\Program Files\CVision\PdfCompressor`*xx*`\` where *xx* stands for the version number of PdfCompressor.
3. Log in to Content Server as an administrator.
4. From the main menu, choose **Administration** then **Admin Applets**.
5. From the Applets list, choose **Configuration Manager**.
6. On the Configuration Manager page, click **Information Fields** tab.
7. If the OCRLang information field has been added, skip this step. If it has not been added:
   a. In the Field Info section, click **Add**.
   b. On the Add Custom Info page, in the Field Name field, enter **OCRLang**. This creates a new information field for CVista language conversion options.

      > **Note:**
      >
      > Enter this field name *exactly*.

   c. Click **OK**.
   d. On the Add Custom Info Field page, in the Field Caption field, enter the descriptive caption to be displayed on the Content check-in Form page. For example, `OCR Language`.
   e. From the Field Type list, choose **Text**.
   f. Select the **Enable Option List** check box.
   g. From the Option List Type list, choose **Select List Validated**.
   h. In the Use option list field, enter `xOCRLangList`.
   i. Click **Edit** next to the Use Option List field.

j. On the Option List page, enter the CVista OCR languages to present as options. The following language names are valid options.

> **Note:**
>
> You can use either the English language name or the native equivalent (if listed). However, you must enter the language options *exactly* as they appear in the following table.

English	Native
Czech	-
Danish	Dansk
Dutch	Nederlands
English	-
Finnish	Suomi
French	Français
German	Deutsch
Greek	-
Hungarian	Magyar
Italian	Italiano
Norwegian	Norsk
Polish	Polski
Portuguese	Português
Russian	-
Spanish	Español
Swedish	Svenska
Turkish	-

k. Select the **Ignore Case** check box.

l. Click **OK**.

m. In the Default Value field, enter the default OCR language option.

n. Click **OK** to save the settings and return to the **Information Fields** tab.

o. Click **Update Database Design**.

8. If the OCRLang Information field has been added, but changes must be made to the languages option list and/or the default language:

a. In the Field Info section, select OCRLang and click **Edit**.

b. On the Add Custom Info page, click **Edit** next to the Use Option List field.

c. On the Option List page, delete any unused CVista OCR languages.

d. Click **OK**.

e. In the Default Value field, enter the default OCR language option.

f. Click **OK** to save the settings and return to the **Information Fields** tab.

9. Close the Configuration Manager applet. When a user checks in a TIFF file, the user can override the default OCR language by selecting any of the OCR languages that were set up.

23.3 Managing XML Conversions

XML conversions require the following components to be installed and enabled on the specified server.

Component Name	Component Description	Enabled on Server
XMLConverter	Enables Inbound Refinery to produce FlexionDoc and SearchML-styled XML as the primary web-viewable file or as independent renditions, and can use the Xalan XSL transformer to process XSL transformations.	Inbound Refinery Server
XMLConverterSupport	Enables Content Server to support XML conversions and XSL transformations.	Content Server

This section discusses the following XML conversion management topics:

- Configuring Content Servers to Send Jobs to Inbound Refinery
- Setting XML Files as the Primary Web-Viewable Rendition
- Setting XML Files as an Additional Rendition
- Setting Up XSL Transformation

23.3.1 Configuring Content Servers to Send Jobs to Inbound Refinery

File extensions, file formats, and conversions are used in Content Server to define how content items should be processed by Inbound Refinery and its conversion add-ons. Each Content Server must be configured to send files to refineries for conversion.

When a file extension is mapped to a file format and a conversion, files of that type are sent for conversion when they are checked into the Content Server. File extension, file format, and conversion mappings can be configured using either the File Formats Wizard or the Configuration Manager.

Most conversions required for Inbound Refinery are available by default in Content Server. In addition to the default conversions, the following conversions are added to the Content Server when the XMLConverterSupport component is installed.

Conversion	Description
FlexionXML	Used to convert files to XML using the FlexionDoc schema. It applies to file types other than the standard file types included in the list of conversions (for example, Word, PowerPoint, and so on). To send these standard file types to a refinery for conversion to XML using FlexionDoc, their file formats do not need to be re-mapped to the FlexionXML conversion. This conversion is not available on the File Formats Wizard. It must be mapped using the Configuration Manager.
SearchML	Used to convert files to XML using the SearchML schema. It applies to file types other than the standard file types included in the list of conversions (for example, Word, PowerPoint, and so on). To send these standard file types to a refinery for conversion to XML using SearchML, their file formats do not need to be re-mapped to the SearchML conversion. This conversion is not available on the File Formats Wizard. It must be mapped using the Configuration Manager.
XSLT Transformation	After XML Converter converts documents to the FlexionDoc schema, the XSLT conversion allows the resultant XML to be transformed into other XML schema specified by a developer.

Conversions available in the Content Server should match those available in the refinery. When a file format is mapped to a conversion in the Content Server, files of that format are sent for conversion on check-in. One or more refineries must be set up to accept that conversion.

Most conversions required for Inbound Refinery are available by default. In addition to the default conversions that can be accepted by a refinery, the FlexionXML and SearchML conversions are added to the refinery when the XMLConverter component is installed. The FlexionXML and SearchML conversions are accepted by default.

23.3.2 Setting XML Files as the Primary Web-Viewable Rendition

To set XML files as the primary web-viewable rendition:

1. Log into the refinery.
2. Choose **Conversion Settings** then select **Primary Web Rendition**.
3. On the Primary Web-Viewable Renditions page, select the **Convert to XML** option.
4. Typically all other conversion options should be cleared. Inbound Refinery attempts to convert each incoming file based on the native file format. If the format is not supported for conversion by the first selected method, Inbound Refinery checks if the next selected method supports the format, and so on. Inbound Refinery attempts to convert the file using the first selected method that supports the conversion of the format.

   For example, suppose you select both the **Convert to PDF using third-party applications** option and the **Convert to XML** option. The refinery attempts to convert any supported formats to PDF using the **Convert to PDF using third-party applications** method. Whether or not this method fails, Inbound Refinery does not attempt another conversion method for these formats. Therefore, you should typically select only the **Convert to XML** option to create XML files as the primary web-viewable rendition.
5. Click **Update** to save all changes.
6. Click **XML Options**.
7. On the XML Options page, set XML options, and click **Update** to save the changes.

8. Note the following important considerations:
   - If you want to adjust the default settings for the Flexiondoc and SearchML options, you can specify option settings in the `intradoc.cfg` file located in the refinery *`DomainDir`*`/ucm/ibr/bin` directory. For a complete description of available Flexiondoc and SearchML options, see the `xx.cfg` file located in the refinery *`IdcHomeDir`*`/components/XMLConverter/resources` directory. You must restart your refinery after making changes to the `intradoc.cfg` file.
   - FlexionDoc and SearchML documentation files are installed with the XMLConverter component and located in the refinery *`IdcHomeDir`*`/components/XMLConverter` directory.

23.3.3 Setting XML Files as an Additional Rendition

To set XML files as an additional rendition:

1. Log into the refinery.
2. From **Conversion Settings**, select **Additional Rendition**s.

   The Additional Renditions page opens.
3. Select the **Create XML renditions for all supported formats** option. Inbound Refinery will generate an XML file in addition to other renditions such as PDF files.

   When the generated XML files are delivered back to a Content Server, the XML files are included in the full-text index. However, if other web-viewable files are generated in addition to the XML file, the XML file is not used as the primary web-viewable rendition. For example, if Inbound Refinery generates both a PDF file and an XML file, the PDF file would be used as the primary web-viewable rendition. XML renditions stored in the Content Server `weblayout` directory can be recognized by the characters `@x` in their file names. For example, the file `Report2001@x~2.xml` would be an XML rendition.
4. Click **Update** to save your changes.
5. Click **XML Options**.
6. On the XML Options page, set your XML options, and click **Update** to save your changes.
7. Note the following important considerations:
   - If you want to adjust the default settings for the Flexiondoc and SearchML options, you can specify option settings in the `intradoc.cfg` file located in the refinery *`DomainDir`*`/ucm/ibr/bin` directory. You must restart your refinery after making changes to the `intradoc.cfg` file.
   - For a complete description of available Flexiondoc and SearchML options, see the `xx.cfg` and `sx.cfg` files located in the refinery *`IdcHomeDir`*`/components/XMLConverter/resources` directory. These configuration files are for reference only and should not be modified.
   - FlexionDoc and SearchML schema code and documentation files are installed with the XMLConverter component into the refinery *`IdcHomeDir`*`/components/XMLConverter` directory.

23.3.4 Setting Up XSL Transformation

Inbound Refinery uses the Xalan XSLT processor and the SAX validator built into the Java virtual machine running Inbound Refinery. To enable transformation, the XMLConverter component must be installed and enabled on the refinery server and the XMLConverterSupport component must be installed and enabled on the Content Server.

To turn on XSL Transformation:

1. Log into the refinery server.
2. Do one of the following:
   - If the XML rendition is to be the primary web-viewable file, click **Conversion Settings** then **Primary Web Rendition**. Enable **Convert to XML** on the Primary Web-Viewable Rendition Page when it is displayed.
   - If the XML is to be an additional rendition, click **Conversion Settings** then **Additional Renditions**. Enable **Create XML renditions for all supported formats** on the Additional Renditions Page when it is displayed.
3. Click **XML Options**.
4. On the XML Options page, enable **Process XSLT Transformation** and select the XML schema to use from the following options:
   - Produce FlexionDoc XML
   - Produce SearchML
5. Click **Update** to save all changes or **Reset** to revert to the last saved settings.

In order to preform XSL transformations Inbound Refinery must have an XSL template to apply during the transformation checked into Content Server. To check in an XSL template to Content Server:

1. Create an XSL file. The XSL file specifies how an XML file with a specific Content Type will be transformed to a new XML file. A DTD or schema can be specified for validation and stored in the Content Server, but is not required.
2. Check the XSL file into the Content Server and associate it to a Content Type.
   a. In the Content check-in Form, select the **Content Type** from the **Type** list.
   b. Enter the Content ID according to the following convention:

      Content Type.xsl

      For example, if the Content Type is `Documents`, enter **documents.xsl**.
   c. Enter the XSL file as the Primary File.
   d. Check that the Security Group matches any DTD/schema files in the Content Server associated with the XSL file and the native files that are checked into the Content Server.
   e. Click **Check In**.

   When files are checked in with this Content Type, and a FlexionDoc/SearchML XML file is generated by XML Converter or the checked-in file is XML, this XSL file will be used for XSL transformation to a new XML document.
3. Repeat these steps for each Content Type to post-process to XML.

23.3.4.1 XSLT Errors

When a validation fails, Inbound Refinery collects the errors from the SAX Validation engine, creates an hcsp error page and attempts to check in the page to Content Server.

Manually set up outgoing providers on Inboard Refinery to the Content Server for the refinery to check in an error page. The name of Inbound Refinery provide must match the agent name. For example if Inbound Refinery is named `production_ibr` and it is converting files for a Content Server named `production_cs`, then an outgoing provider named `production_cs` must be created on the `production_ibr` Inbound Refinery.

To set up a criteria workflow to be notified regarding XSL transformation failures:

1. From the main menu, choose **Administration** then **Admin Applets.**
2. From the Applet list, choose **Workflow Admin**.
3. Add a criteria workflow for notification of XSLT transformation failures.
4. Add a workflow step with the following properties:

- **Users**: specify the users that should be notified.
- **Exit Conditions**: select **At least this many reviewers**, and set the value to 0.
- **Events**: For the **Entry** event, add the following Custom Script Expression:

```
<$if dDocTitle like "*XSLT Error"$>
<$else$>
<$wfSet("wfJumpEntryNotifyOff", "1")$>
<$wfExit(0,0)$>
<$endif$>
```

For details about using workflows, see Managing Workflows.

23.4 Converting Microsoft Office Files to HTML

Inbound Refinery can convert native Microsoft Office files to HTML by using the native Microsoft Office applications installed on a Windows system. Content Server can be installed on either a Windows or UNIX platform, but for Microsoft Office to HTML conversions to work, Inbound Refinery must be configured on the Windows system where the Microsoft Office native applications are installed.

HTML conversion automates opening Microsoft office files in their native application, saves them out as HTML pages, then collects the HTML output into a compressed ZIP file that gets returned to Content Server.

HTML conversion can process the following types of files:

- Microsoft Word 2003 through 2010
- Microsoft Excel 2003 through 2010
- Microsoft PowerPoint 2003 through 2010
- Microsoft Visio 2007

When WinNativeConverter is enabled to work with Inbound Refinery, native Microsoft Office files checked into Content Server are sent to Inbound Refinery for conversion. Inbound Refinery automates the process of converting the files to HTML using the

native Microsoft Office applications. If a single HTML page is returned to Content Server, it is used as the web-viewable file. If conversion results in multiple HTML pages, the following files are returned to Content Server:

- An HCSP page as the primary web-viewable rendition
- A ZIP file that includes the HTML output from the Office application
- Optionally, a thumbnail rendition of the native Microsoft Office file

When a user clicks on the web-viewable link in Content Server of a document converted to multiple HTML pages by Inbound Refinery, the HCSP page redirects the server to the HTML rendition.

Microsoft Office to HTML conversions require the following components to be installed and enabled on the specified server.

Component Name	Component Description	Enabled on Server
WinNativeConverter	Enables Inbound Refinery to convert native Microsoft Office files created with Word, Excel, PowerPoint and Visio to HTML using the native Office application.	Inbound Refinery Server
MSOfficeHtmlConverterSupport	Enables Content Server to support HTML conversions of native Microsoft Office files converted by Inbound Refinery and returned to Content Server in a ZIP file. Requires that ZipRenditionManagement component be installed on the Content Server.	Content Server
ZipRenditionManagement	Enables Content Server access to HTML renditions created and compressed into a ZIP file by Inbound Refinery.	Content Server

This section discusses how to configure Content Server to work with Microsoft Office to HTML conversions:

- Configuring Content Servers to Send Jobs for HTML Conversion

23.4.1 Configuring Content Servers to Send Jobs for HTML Conversion

When installed on the refinery, the WinNativeConverter adds the Word HTML, PowerPoint HTML, Excel HTML, and Visio HTML option to the Conversion Listing page. This conversion option must be enabled for the refinery to perform conversions on items submitted by the Content Server. File formats and conversion methods are used in Content Server to define how content items should be handled by Inbound Refinery and the conversion options.

For a Microsoft Office document to be processed by Inbound Refinery, its file extension must be mapped to a format name that is associated with the HTML Conversion method. The added conversion options for HTML Conversion are not automatically mapped: they must be mapped manually. They can be set either using the File Formats Wizard or the Configuration Manager applet. The Configuration Manager applet gives you greater control over which file extensions are mapped to which conversion options. For details, see the following sections:

- Using the File Formats Wizard for Microsoft Office Conversions
- Using the Configuration Manager for Microsoft Office Conversions

23.4.1.1 Using the File Formats Wizard for Microsoft Office Conversions

File formats and conversion methods for Inbound Refinery can be managed in Content Server using the File Formats Wizard. To make changes:

1. Log in to Content Server as an administrator.
2. From the main menu, choose **Administration** then **Refinery Administration** then **File Formats Wizard**.
3. On the File Formats Wizard, select the Microsoft Office document file types you want to convert to HTML. The Conversion column lists the appropriate conversion option according to the file type. For example:
   - **Word** for doc, docx, dot, dotx
   - **PowerPoint** for ppt, pptx
   - **Excel** for xls, xlsx
   - **Visio** for vsd

   > **Note:**
   >
   > HTML conversion can process the following types of files:
   > - Microsoft Word 2003 through 2010
   > - Microsoft PowerPoint 2003 through 2010
   > - Microsoft Excel 2003 through 2010
   > - Microsoft Visio 2007

4. Click **Update** to save all changes.
5. Log in to the Inbound Refinery as an administrator.
6. From the navigation menu, choose **Conversion Settings** then **Primary Web Rendition**.
7. On the Primary Web Rendition page, enable **Convert selected MS Office formats to MS HTML**.
8. Click **Update**.

23.4.1.2 Using the Configuration Manager for Microsoft Office Conversions

File formats and conversion methods for Inbound Refinery can be managed in Content Server using the Configuration Manager. To make changes:

1. Log in to Content Server as an administrator.
2. From the main menu, choose **Administration** then **Admin Applets**.
3. From the Applet list, choose **Configuration Manager**.
4. Choose **Options** then **File Formats**.

5. Select the application format for the Office document type to convert from the **Format** column. For example, for Microsoft Word, select **application/msword**.
6. Click **Edit**.
7. In the Edit File Format dialog, select the HTML conversion option from the **Conversion** list appropriate to the selected Office document format. For example, for **application/msword**, select the conversion option **Word HTML**.
8. Click **OK**.
9. Repeat these steps for all Microsoft Office formats to convert to HTML.
10. When finished, click **Close** to close the File Formats page and then close the Configuration Manager.
11. Restart Content Server and Inbound Refinery.

24

Working With Image and Video Conversions

The Digital Asset Manager feature is used to define and provide images, videos, and audio files in specified formats and sizes for download by the people in your organization who need them. This helps organizations maintain consistent standards for branding and digital content use.

For Digital Asset Manager to work, the following components must be installed and enabled on the correct server as noted.

Component Name	Component Description	Enabled on Server
DAMConverter	Enables Oracle WebCenter Content: Inbound Refinery to convert digital assets into multiple renditions.	Inbound Refinery Server
DamConverterSupport	Enables the Content Server to support digit asset management features. This component is highly dependent on the ZipRenditionManagement Component.	Content Server
DigitalAssetManager	Enables the user interface for digital asset management in tight integration with components used to create and manage renditions and zip file archives. This component is highly dependent on the ContentBasket Component.	Content Server
ContentBasket	Enables users to select renditions of content items and place them in a personal storage space called the Content Basket.	Content Server
ZipRenditionManagement	Enables Content Server access to digital asset renditions created and compressed into a ZIP file by Inbound Refinery.	Content Server

This section discusses the following topics:

24.1 Understanding Digital Asset Manager

Digital Asset Manager creates multiple formats of digital assets automatically when an image or video is checked into Content Server, and lists the formats under one content ID. This ensures that the asset, such as a corporate logo or promotional video, maintains a standard size and quality in the multiple formats required by an organization, while providing the content management features of Content Server. For example, one person can bundle and download images of the logo for use on a web-site, and another can download and bundle images of the same logo for use in office presentations or print collateral, all from a single digital asset checked into Content Server.

Digital assets are valuable electronic images and videos to be made available within an organization in multiple output formats, called renditions. The quantity and type of renditions are defined by the system administrator in rendition sets. A user selects a rendition set used to create renditions of a digital asset at the time the asset is checked into Content Server. Once checked in, a digital asset is routed to Inbound Refinery and converted using the specified conversion application.

This section discusses the following topics:

- Supported Conversion Applications
- Supported Streaming Servers
- Supported Input Formats
- Supported Output Formats

24.1.1 Supported Conversion Applications

By default, Inbound Refinery supplies rendition sets for use with Oracle Outside In Image Export to convert images. For additional image conversion options, a stand-alone graphics conversion application can be installed. Oracle does not supply or support any specific third-party conversion engine. Sample configurations for additional image conversion engines can be accessed from the Oracle WebCenter Content Oracle Technology Network pages. For additional information, see the "Integrating the Inbound Refinery with 3rd Party Image Converters" blog.

To convert videos, a stand-alone video conversion application must be installed. Digital Asset Manager is currently configured to work with Telestream's Vantage. A supported version of Vantage must be obtained from Telestream and is available from their website (`http://www.telestream.net`).

Digital Asset Manager is designed and tested on fully functioning implementations of third-party conversion applications. Demonstration versions of conversion applications are not recommended or supported.

24.1.2 Supported Streaming Servers

For streaming digital video, Digital Asset Manager currently supports the following streaming servers:

- Windows Streaming Media: versions for supported Windows operating systems

- QuickTime Streaming Media: Darwin and QuickTime Streaming Server version 10.4
- RealMedia: Helix DNA Server version 11

24.1.3 Supported Input Formats

Supported input formats are determined by the graphic or video conversion application being used. Digital Asset Manager can use several graphic conversion engines. Only Oracle Outside In Image Export is included with Inbound Refinery. Formats supported by Oracle Outside In Image Export can be found on Oracle's website at http://www.oracle.com/technetwork/middleware/webcenter/content/oit-all-085236.html.

Third-party conversion engines may offer additional support to graphics format. Third-party conversion engines must be obtained independently of Inbound Refinery and are not officially supported by Oracle.

Graphics formats supported by compatible conversion engines include the following:

- JPG/JPEG (Joint Photographic Expert Group)
- GIF (Graphics Interchange Format)
- BMP (Bitmap)
- PNG (Portable Network Graphics)
- TIFF (Tag Image File Format)
- PSD (PhotoShop)
- AI (Adobe Illustrator)
- PDF (Portable Document Format)

For a comprehensive listing of formats supported, view the documentation that came with your chosen graphic conversion engine.

24.1.4 Supported Output Formats

Output formats are determined by the conversion application. Formats supported by Oracle Outside In Image Export can be found on Oracle's website at http://www.oracle.com/technetwork/middleware/webcenter/content/oit-all-085236.html.

Viewing of renditions in your browser is limited to what can be displayed effectively in your browser. For images, only formats supported by your web browser can be displayed. For video, only formats that have browser plug-ins are available for viewing in your web browser, such as output formats supported by Windows Media Player, Real Player, QuickTime Player, and Flash. Any image or video assets rendered in a format not supported for viewing in a browser will still be managed by Content Server, but will be available only for download.

Video Manager currently supports the following output formats:

- MPEG Layers 1, 2, and 4 (.mpg, .mpeg, .mp2, .mp4)
- MPEG Layer 3 Audio (.mp3)
- Adobe Flash (.flv)
- QuickTime (.mov)
- Audio Video Interleave (.avi)

Due to the extensive number of formats supported by Telestream's Vantage, Windows Media Player, Real Player, QuickTime Player, and Adobe Flash, and the difficulty in configuring all the possible combinations, Video Manager officially supports a limited subset of these formats. You can configure Digital Asset Manager to accept additional formats and test them as needed.

> **Note:**
>
> If using Microsoft IIS to serve conversions, unrecognized MIME types generate a 404 error. To ensure that the browser properly displays supported formats, check that all MIME types being used are registered in IIS.
>
> For more information, see the IIS documentation and the Microsoft article at `http://technet.microsoft.com/en-us/library/cc725608%28WS.10%29.aspx`.

24.2 Configuring Digital Asset Manager

The following configuration files must be modified to configure Digital Asset Manager for image and video conversion:

- Content Server `config.cfg` file, located in the *`IntradocDir`*`/config/` directory
- Inbound Refinery `intradoc.cfg` file, located in the *`DomainDir`*`/ucm/ibr/bin` directory

This section details the necessary configuration steps.

- Configuring for Image Conversion
- Modifying the Content Server Configuration File
- Associating File Formats and Mapping File Extensions
- Associating a File Format
- Mapping File Extensions

24.2.1 Configuring for Image Conversion

Digital Asset Manager requires a conversion application to create renditions of an image. Default rendition sets for use with Oracle Outside In Image Export are provided and no configuration is necessary.

Default Rendition Sets

Default rendition sets are defined in the `damconverter_basedefinitions.hda` file, which is located in the refinery *`IdcHomeDir`*`/components/DAMConverter/resources/` directory. This file should never be altered because upgrades to the component overwrite any changes. For information about defining and using rendition sets other than the default sets included in the `damconverter_basedefinitions.hda`, see Creating and Configuring Image Rendition Sets.

The following default rendition sets are included in the `damconverter_basedefinitions.hda` file installed with Digital Asset Manager.

Rendition Set Name	Description
ThumbnailOnly	Creates one 72 dpi PNG rendition exactly 80 pixels high
BasicRenditions	Creates the following renditions: • **Web**: A JPEG rendition no bigger than 800 x 600 pixels • **Thumbnail**: A PNG rendition exactly 80 pixels high • **Preview**: A GIF rendition exactly 250 pixels wide
MultipleFormats	Creates the following renditions: • **Web**:A JPEG rendition no bigger than 800 x 600 pixels • **Thumbnail**: A PNG rendition exactly 80 pixels high • **Preview**: A GIF rendition of the original file with no parameters specified • **Jpeg2000**:A JPEG 2000 rendition no bigger than 800 x 600 pixels wide • **Tiff**: A TIFF rendition with no parameters specified. When no parameters are specified, the dpi and pixel size of the original file is maintained. • **Bitmap**: A BMP rendition with no parameters specified

Alternate Conversion Applications

If needed, an alternate conversion application can be used. To use a conversion application other than Oracle Outside In Image Export, obtain and install the application and define rendition sets suitable for the application.

> **Note:**
>
> For best performance rendering images, install the image conversion application on the same server as the Inbound Refinery instance used for Digital Asset Manager. For best performance rendering videos, see the recommendations of the video conversion application.

Additional rendition sets should be defined in a new file called `extraRendition_definitions.hda` which must be created in the `/data/configuration/dam/` directory. For information about creating additional rendition sets, see Creating and Configuring Image Rendition Sets.

24.2.2 Modifying the Content Server Configuration File

A default value must be set for the VideoRenditions and ImageRenditions metadata fields to prevent errors if a rendition set is not selected at time of check-in. To modify the configuration file:

1. Open the *`IntradocDir`*`/config/config.cfg` file in a standard text editor.
2. In the #Additional Variables section, add `DefaultVideoConversionSet` for video and `DefaultPackedConversionSet`.
3. For video, set `DefaultVideoConversionSet` equal to the factory to use as the default rendition set. For images, set it to your preferred rendition set.

> **Note:**
>
> The selected default must match a rendition set in the choice list of the VideoConversions or ImageRenditions metadata field, defined using the Configuration Manager applet.

4. Save the changes and close the file.
5. Restart Content Server

Digital Asset Manager allows a user to bundle and download assets to a local or shared file system. Edit the following variables to set the maximum allowable size of a download can be specified, either in megabytes or number of files:

- `MaxRenditionBundleInMegabytes`=Maximum size of bundle in megabytes.
- `MaxRenditionFileEntries`=Maximum number of files in the bundle, expressed numerically.

> **Note:**
>
> The `DefaultVideoConversionSet` identifies the rendition set to be used if a user does not specify a video rendition set when checking in a video. The `DefaultPackedConversionSet` identifies the rendition set to be used if a user does not specify an image rendition set when checking in an image. They must be set in the `config.cfg` file, and not in the Default Value field of the Content Manager applet.

24.2.3 Associating File Formats and Mapping File Extensions

Content Server identifies content items as digital assets based on the extension of the file checked in. The following file formats must be associated with Digital Asset Manager and the file extensions mapped to the correct format.

24.2.3.1 Image Formats

- JPEG (.jpeg; .jpg)
- GIF (.gif)
- AI (.ai)
- PSD (.psd)
- BMP (.bmp)
- PNG (.png)
- TIFF (.tiff; .tif)

24.2.3.2 Video Formats

- MPEG Layers 1, 2, and 4 (.mpg, .mpeg, .mp2, .mp4)
- QuickTime (.mov)

- Audio Video Interleave (.avi)
- Flash Video (.flv)

Because the conversion engine passes rendition information to the third-party conversion application, any additional format must be supported by the third-party conversion application.

> **Note:**
>
> When converting one type of digital asset, images or videos, only associate the formats for that type of asset.

24.2.4 Associating a File Format

To associate a format with the Digital Asset Manager conversion engine:

1. Log in as an administrator to Content Server.
2. From the main menu, choose **Administration** then **Admin Applets**.
3. From the Applets list, choose **Configuration Manager**.
4. On the Configuration Manager applet, choose **Options** then **File Formats**.
5. On the File Formats page, associate the format with the Digital Asset Manager conversion engine.

   If the format is listed in the File Formats (upper) section of the File Formats page:

   a. Select the format from the list. For example select, `image/jpeg` for JPEG images or `video/mpeg` for MPEG videos.

   b. Click **Edit**.

   c. On the Edit File Format page, select **Digital Media Graphics** for image formats and **Digital Media Video** for video formats from the Conversion choice list. Digital Media Graphics and Digital Media Video are the names of the Digital Asset Manager conversions.

   d. If needed, modify the description. The description is displayed in the Configuration Manager and is not displayed in the Content Server interface.

   e. Click **OK**.

   If the format is not listed in the File Formats (upper) section of the File Formats page:

   a. Click **Add**.

   b. On the Add New File Format page, enter the type of format in the Format field. The type can be any value and is displayed on the Content Information and Rendition Information pages of Content Server. For help in choosing the correct type, see Identifying MIME Types.

   c. Select **Digital Media Graphics** for images or **Digital Media Video** for videos from the Conversion choice list. Digital Media Graphics and Digital Media Video are the names of the Digital Asset Manager conversions.

   d. If needed, add a description. The description is displayed in the Configuration Manager and is not usually displayed in the Content Server interface.

The description can be displayed in the user interface if the configuration variable `IsOverrideFormat` is set equal to true in the Content Server configuration file. Setting `IsOverrideFormat=true` in the Content Server configuration file enables a choice list on the check-in page that allows a user to select a conversion format for a specific file, bypassing the assigned format.

e. Click **OK**.

24.2.5 Mapping File Extensions

After a format is associated with the appropriate Digital Media conversion engine, the appropriate file extensions must be mapped to the file format in Configuration Manager. All files with a file extension mapped to a format associate with Digital Media Graphics or Digital Media Video are sent to Inbound Refinery for conversion.

To map a file extension to a file format associated with the Digital Asset Manager conversion engine:

1. Log in as an administrator to Content Server.
2. From the main menu, choose **Administration** then **Admin Applets**.
3. From the Applets list, choose **Configuration Manager**.
4. Choose **Options** then **File Formats**.
5. On the File Formats page, map the extensions to the appropriate format:

   If the extension is listed in the File Extensions (lower) section of the File Formats page:

   a. Select the extension from the list.
   b. Click **Edit**.
   c. On the Edit File Extension page, select the appropriate format from the **Map to Format** choice list.
   d. Click **OK**.

   If the format is not listed in the File Formats (upper) section of the File Formats page:

   a. Click **Add**.
   b. On the Add File Extensions page, enter the file extension in the **Extension** field. Do not enter the dot of the file extension.
   c. Select the appropriate format from the **Map to Format** choice list.
   d. Repeat steps a through c for each extension to be associated with the format. For example, `pspimage` could also be associated with `application/PaintShop`.
   e. Click **OK**.
   f. Click **Close**.
   g. Close Configuration Manager.

   After associating a format to the appropriate Digital Asset Manager conversion (Digital Media Graphics or Digital Media Video), and mapping the appropriate file extensions to the format, all files with those extensions checked into Content Server are passed to Inbound Refinery for processing through the conversion application.

24.3 Setting Up and Managing Image Conversions

This section discusses the following topics:

- Understanding Image Rendition Sets
- Creating and Configuring Image Rendition Sets
- Working with XMP and EXIF Data

24.3.1 Understanding Image Rendition Sets

When a digital asset is checked in to Content Server, Digital Asset Manager creates multiple renditions of that asset. The criteria for each image rendition is defined in one of two files.

The default renditions set is defined in the `damconverter_basedefinitions.hda` file and it should not be modified. Custom rendition sets can be added to the `extraRendition_definitions.hda` component resource file. This file can be created with a standard text editor and must be located in a new directory named `dam` in the refinery *`IntradocDir`*`/data/configuration/` directory. The full file path should be:

`IntradocDir``/data/configuration/dam/extraRendition_definitions.hda`

For videos, the criteria is defined in the video conversion application.

24.3.1.1 About Image Asset Rendition Definition

The criteria defining the default rendition sets at installation are in the `damconverter_basedefinitions.hda` file in the *`IdcHomeDir`*`/components/DAMConverter/resources/` directory. This file should not be edited.

The definitions are grouped into rendition sets which correspond to rendition sets available to contributors on the content check-in form when a image asset is checked in. It includes the following predefined rendition sets:

- ThumbnailOnly
- BasicRenditions
- MultipleFormats

The included rendition sets are examples that work with Outside In Image Export. If they are not needed, remove them from the option list on the check-in page using the Configuration Manager. Do not edit the resource file to remove the sets. Any changes made are lost when a component is updated.

Additional rendition sets can be added the extraRendition_definitions.hda file, which can be created with a standard text editor. It must be stored in a new directory named `dam` in the refinery *`IntradocDir`*`/data/configuration/` directory.

Digital Asset Manager merges `damconverter_basedefinitions.hda` and `extraRendition_definitions.hda` when running, with the second file taking precedence over the resource file. For example, if you create a new rendition in your file with the same name as one in the resource file but with different parameters, the new parameters are used.

24.3.1.2 About Defining Image Rendition Sets

When a contributor checks a digital asset into Content Server, a rendition set is selected on the check-in form. For image files, that rendition set matches a rendition set defined in either the `damconverter_basedefinitions.hda` file or the `extraRendition_definitions.hda` file.

Image rendition sets defined in the `extraRendition_definitions.hda` file contain the options for converting digital assets into the image renditions specified in the set. The default renditions sets are in the component resource file, which should not be changed. Any additional rendition sets should be added to the `extraRendition_definitions.hda`. In that file, the top properties section contains the file path to a third-party conversion application. The bottom section contains the rendition set options, organized into sets, called rendition result sets.

When a file is checked into Content Server, the format of the file determines if it is a digital asset. If it is an image file, Content Server passes the file to Inbound Refinery, which calls rendition options from the `extraRenditions.hda` file and pass them to the image conversion application. The resulting renditions are then passed back through Inbound Refinery to Content Server or other specified location, where they are managed under a single content ID and made available to your organization.

For image assets, the names of the rendition sets defined for the choice list in the PackagedConversions metadata field in the Configuration Manager applet must match exactly to the names of the rendition sets defined in the `extraRendition_definitions.hda` file.

When modifying or adding renditions, it is important to remember that a contributor will only see the name of the rendition set when checking in a digital asset. The rendition set name should be descriptive. Rendition names and descriptions are displayed on the content information and rendition information pages.

Spaces and other characters reserved for Idoc Script tags or are illegal for use in URLs, such as spaces, cannot be used in rendition names.

24.3.2 Creating and Configuring Image Rendition Sets

To add, modify, or delete image renditions and rendition sets, edit the *`IntradocDir`*`/data/configuration/dam/extraRendition_definitions.hda` file. To successfully modify the `extraRendition_definitions.hda` file, you should be aware of basic HDA file structure. For more detailed information, see *Developing with Oracle WebCenter Content*.

This section discusses the following topics:

- extraRendition_definitions.hda File Structure
- Adding a Rendition Set
- Enabling a Rendition Set

24.3.2.1 extraRendition_definitions.hda File Structure

When defining additional rendition sets, the `extraRendition_definitions.hda` file must contain a header line and two section types.

Section Types

The `extraRendition_definitions.hda` file has two section types using the following format:

```
@section_type section_name
Section data
@end
```

The two section types are:

- Properties Section
- ResultSet Section

In the `extraRendition_definitions.hda` file, there is one properties section and multiple result set sections. All rendition sets are organized in result sets.

Comments are not allowed within a section of an HDA file. However, comments can be placed in the HDA file before the first section, between sections, or after the last section.

Blank lines within a section of an HDA file are interpreted as a NULL value. Blank lines before the first section, between sections, or after the last section are ignored.

Properties Section

The properties section of the `extraRendition_definitions.hda` file defines the path to an external conversion application. In the default file, it also declares the values of Idoc Script variables defining conversion options used by the default rendition result sets.

Default Idoc Script variables in the properties section are used by the default rendition sets. They are not required for any additional rendition sets you define and are not discussed in this guide. Conversion options can be specified directly within the result sets. For more information on working with Idoc Script, see *Developing with Oracle WebCenter Content*.

Result Set Sections

Two types of result sets are in the `extraRendition_definitions.hda` file, listed here in order of display in the file:

- Rendition Result Sets
- ExtensionFormatMap

Rendition result sets organize rendition sets and contain information about creating renditions. There can be many rendition result sets, in any order. They can be added, modified, or deleted, but each name must be unique.

The ExtensionFormatMap is an optional result set that lists file extension/format pairs, so Inbound Refinery can return the correct file format to Content Server for use internally. This is not a required set, as Inbound Refinery uses a different system to map extensions to mime types, but if this result set is defined, the mapping specified in it takes precedence.

24.3.2.2 Adding a Rendition Set

The simplest way to add a rendition set to the `extraRendition_definitions.hda` file is to copy an existing rendition result set and modify it. To successfully modify an existing set, be aware of basic set structure.

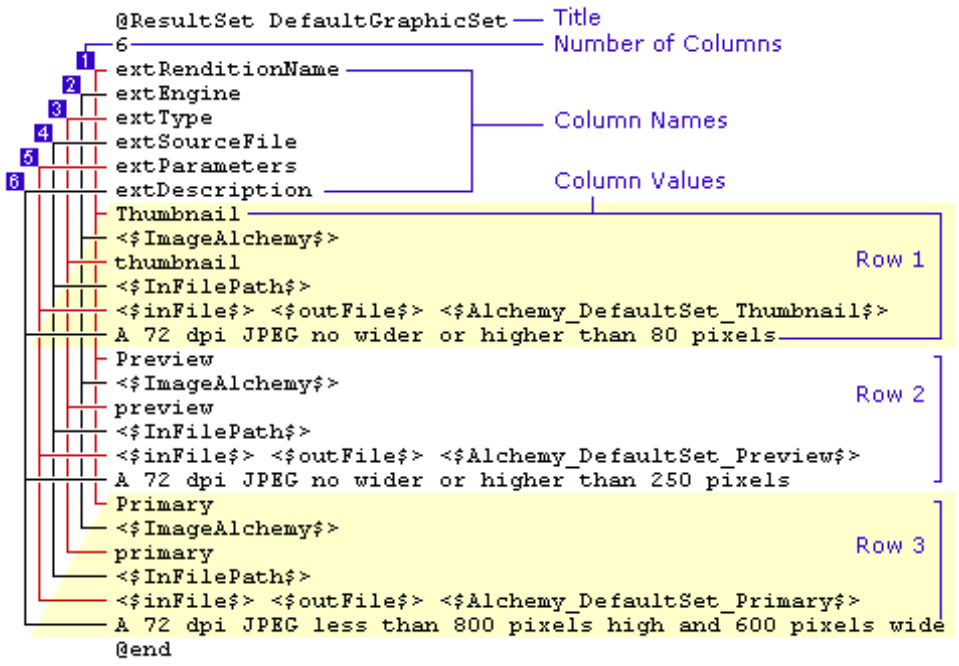
Modifications made to a component resource such as `damconverter_basedefinitions.hda` are overwritten if Digital Asset Manager is updated to a newer version. Do not edit the

`damconverter_basedefinitions.hda` manually. Additional rendition sets should be added to the `extraRendition_definitions.hda` file created in the *`IntradocDir`*`/data/configuration/dam`. Digital Asset Manager uses both files when running.

Rendition Result Set Structure

HDA files are ordered using simple name/value pairs, representing tabular data in an ASCII text format. The first line of a ResultSet section declares the set with the command @ResultSet, and then specifies the name of the set. The second line specifies the number of columns in a table, and the following lines name and populate the columns based on their order in the result set. The last line closes the result set with the command `@end`.

For example, the SampleGraphicSet rendition result set has the following format:



The first line of the rendition result set declares it as a result set by starting with `@ResultSet`, and the last line closes the set, with `@end`. The first line also gives the set a name. In this case, the name is ThumbnailOnly.

The name used should be descriptive, but spaces and other characters reserved for Idoc Script tags or illegal for use in URLs, such as spaces, cannot be used in rendition names.

The second line identifies how many columns are in the result set. In rendition result sets for Digital Asset Manager, there are 6 columns.

Each column has the following name and description.

Column Name	Column Description
extRenditionName	The name of the rendition displayed on the Rendition Information page. This can be any descriptive name. Do not use **Primary** or **Alternate** for rendition names. These terms are reserved for internal use by Content Server.
extEngine	The path to the conversion engine used. By default, this is expressed as an Idoc Script variable declared in the properties section of the extraRendition_definitions.hda file. If you are using Image Export to create the rendition, use `ImageExport` in this column.
extType	How the rendition is being used. • **Thumbnail**: Used on the Thumbnail view of a search results page. • **Preview**: Used on the Rendition Information page. • **Web**: The web-viewable version of a content item. Displayed in the main content area when accessed by clicking the content ID or thumbnail from a search results page, or when clicking the web-viewable link on a content information page. Displayed in a new browser window when accessed by clicking the Preview image on a Rendition Information page. If no web rendition is defined the native file is used by Content Server as the web-viewable file. • **Extra**: Any rendition not defined as Thumbnail, Preview, or Web.
extSourceFile	The file path to the asset checked into for conversion expressed as Idoc Script.

extParameters	The options passed to the conversion engine defining how the source file is rendered. By default, this is expressed as Idoc Script variables declared in the properties section of the extraRendition_definitions.hda file, but it can be expressed as a literal string.
	• **<$infile$>**: The name of the source file used to generate the rendition, expressed as Idoc Script.
	• **<$outfile$>**: The name of the rendered file. This is a required parameter, expressed as Idoc Script.
	• **<$parameter_variable$>**: The options used for rendering by the conversion application. In the provided rendition sets, these are expressed as Idoc Script variables, which are declared in the properties section of the extraRendition_definitions.hda file. They can also be expressed as a literal string of options used by your conversion application. For example, the literal string used in the damconverter_basedefinitions for the Web rendition is:
	`outputid=FI_GIF, graphicoutputdpi=72, graphicwidthlimit=250, graphicheightlimit=0`
	but it could also be expressed as the following variable:
	`<$ImageExport_BasicRenditions_Web$>`
	if the properties section of extraRendition_definitions.hda file sets `ImageExport_BasicRenditions_Web=outputid=FI_GIF, graphicoutputdpi=72, graphicwidthlimit=250, graphicheightlimit=0`

extDescription	The description for the rendition displayed on the Rendition Information page.

For more information about working with `.hda` files, see *Developing with Oracle WebCenter Content*.

To add a new rendition result set:

1. Open the `extraRendition_definitions.hda` file in a standard text editor.
2. Copy and paste an existing rendition result set.
   a. Select a rendition result set to copy, starting at the `@ResultSet` line and ending at the `@end` line, and copy it.
   b. Position the cursor between any two existing rendition result sets in the `extraRendition_definitions.hda` file.
   c. Paste the rendition result set into the file.

   Blank lines between result set sections are ignored. To help visually organize the `extraRendition_definitions.hda` file, it is useful to insert a blank line before and after the new rendition result set.
3. Change the name of the new rendition result set, listed next to `@ResultSet`. For example, `@ResultSet NewName`.

   The name used should be descriptive. Do not use spaces or other characters reserved for Idoc Script tags or which are illegal for use in URLs, such as spaces.
4. Change rendition information for each rendition to keep in the result set.
   a. Change the name of the rendition, listed in the extRenditionName column. Rendition names may have spaces.
   b. Change the type of the rendition, listed in the extType column. Each rendition can multiple types, for example, preview, web.
   c. Change the conversion options for rendering, listed in the extParameters column. Conversion options are dependent on which third-party conversion application being used.
   d. Change the description of the rendition, listed in the extDescription column. The description can be anything, and is displayed on the Rendition Information page.

      Do not change the `<$InFilePath$>` variable used in the extSouceFile column.
5. Delete any extraneous renditions in the result set.
6. Save the `extraRendition_definitions.hda` file.

24.3.2.3 Enabling a Rendition Set

After a rendition set is added to the `extraRendition_definitions.hda` file, it must be made available as an option in the Image Rendition Set field on the Content check-in Form, using Configuration Manager.

To add the name of the rendition set as an option in Configuration Manager:

1. Log in as an administrator to Content Server.
2. Choose **Administration** then **Admin Applets** from the Main menu.
3. Choose **Configuration Manager** from the Applet list.
4. On the **Information Fields** page, select the **PackagedConversions** information field and click **Edit**.
5. Click **Configure**.

6. On the Configure Option List page, click **Edit**.
7. Add the name of the new result set as it is listed in the `extraRendition_definitions.hda` file's packedConversion result set. Rendition sets can be listed in any order.

   The name used in the `extraRendition_definitions.hda` file and the PackagedConversions option list must match. Spaces and other characters reserved for Idoc Script tags or which are illegal for use in URLs cannot be used.
8. Click **OK** to close the Option List page.
9. Click **OK** to close the Configure Option List page.
10. Click **OK** to close the Edit Custom Info page.

24.3.3 Working with XMP and EXIF Data

Most digital images have data associated with them by the hardware or software used to create them. For example, digital photographs have the date they were created and the camera used to create them associated with them, among other things. Digital files such as those created with Adobe Photoshop have a greater set of metadata associated with them. The metadata associated with digital photographs is called EXIF data, which stands for Exchangeable Image File Format. It is a subset of the type of data created by computer applications such as Adobe Photoshop. The application metadata is called XMP data, which stands for EXtensible Metadata Platform.

By default, Inbound Refinery is now configured to send EXIF and XMP data to Content Server, where it is indexed and available for searching as text.

24.3.3.1 Searching XMP and EXIF Data in Content Server

By default, XMP schema and EXIF data are extracted by Inbound Refinery and passed to Content Server. Content Server then displays the data on the **Image Data** tab of a digital asset.

If OracleTextSearch is installed and enabled, the data is indexed and available for searching through a full-text search. To enable searching on a specific criteria in the XMP or EXIF metadata, a placeholder field must be enabled on the Content Server user interface and the search collection must be rebuilt. When done, users can search for content using the specific criteria in the data.

To enable an XMP or EXIF data field on the user interface and make the specific criteria available for searching:

1. Choose **Administration** then **DAM Administration** from the Main menu.
2. On the DAM Search Fields Administration page, expand the section under the XMP Schema Categories that has the data field to enable on the user interface. For example, to search for digital images based on the date and time the image was take, expand the EXIF category.
3. Find and enable the placeholder field to be used for searching. For example, in the EXIF category, scroll to the **XMP Date Time Original** and select it.
4. Click **Update**.
5. Rebuild the search index. For information on rebuilding the search index, see the Oracle WebCenter Content documentation.

> **Note:**
>
> Enabling a field in the user interface creates a placeholder field in Content Server and allows the information to be indexed and searched against. It does not modify database tables or allow information to be entered or modified in the field for storage in the database.

24.4 Setting Up and Managing Video Conversions

Digital Asset Manager requires a third-party conversion application to render video assets checked in to Content Server. Digital Asset Manager is designed to work with Telestream's Vantage (http://www.telestream.net/vantage/overview.htm). You can also use command-line interface tools to create video rendition sets.

This section has the following topics:

- Installing Vantage
- Setting the Shared Directory Path for Vantage
- Setting Media Locations
- Using Streaming Servers
- Defining Video Rendition Sets
- Importing the WindowsMediaWorkflow.xml File
- Understanding the Vantage Workflow
- Managing Video Conversion
- Using the Command-Line Interface (CLI) Tool for Video Rendition Sets

24.4.1 Installing Vantage

The instructions to install Vantage are available on the Telestream website.

Visit http://www.telestream.net/ for information on how to install Vantage.

> **Note:**
>
> Visit http://www.telestream.net/ for the latest information relating to Vantage.
>
> Due to the demand on computer resources required for rendering video assets, it is recommended that Vantage and Inbound Refinery be installed on separate server-class systems. For ease of access, it is also recommended that both servers have a duplicate user list of administrators.
>
> The Vantage license must include:
>
> - Metadata handling
> - Closed captioning handling and analysis
> - Any in or out transcoding requirements

24.4.2 Setting the Shared Directory Path for Vantage

1. Open the *DomainDir*/ucm/ibr/bin/intradoc.cfg file for each Inbound Refinery connection accessing the shared directories in a standard text editor.
2. Add the WatchedWorkflowRootDir variable and set it equal to the path of the workflow directory shared with Vantage. For example:WatchedWorkflowRootDir=\\\\VantageServer\\DAMRenditions\\ . The path can be a local, mapped, or a Universal Naming Convention (UNC) path. The backslash is an escape character in Java, so any path using a backslash must be escaped using two backslashes. For example, the path \\VantageServer\\DAMRenditions\\ becomes \\\\VantageServer\\DAMRenditions\\

   The path to the directories must not contain spaces.
3. Save changes and close the intradoc.cfg file.

If you have three Vantage workflows: WMV, WebSmall, and WebBig, create the following directories:

- For WMV:

  The Watch action should watch: \\\\VantageServer\\DAMRenditions\\WMV\in\

  The Deploy action should deploy to: \\\\VantageServer\\DAMRenditions\\WMV\out\
- For WebSmall:

  The Watch action should watch: \\\\VantageServer\\DAMRenditions\\WebSmall\in\

  The Deploy action should deploy to: \\\\VantageServer\\DAMRenditions\\WebSmall\out\
- For WebBig

  The Watch action should watch: \\\\VantageServer\\DAMRenditions\\WebBig\in\

  The Deploy action should deploy to: \\\\VantageServer\\DAMRenditions\\WebBig\out\

24.4.3 Setting Media Locations

By default, Content Server uses the `weblayout` directory as the media location. This only requires setting a configuration variable in Inbound Refinery to point to the Content Server `weblayout` directory in order to use it as the media location for video.

However, video renditions can be placed in a variety of locations, such as the Content Server `weblayout` directory, placed on a file system for access outside of Content Server, or sent to a streaming server.

> **Note:**
>
> When streaming rendered videos, install and configure a supported media server based on the instructions from the media server, and set the conversion application to deliver the correct streaming format. Currently Digital Asset Manager supports Darwin Streaming Server (QuickTime), Helix Streaming Server (HelixMedia), and Windows Media Server

This section discusses the following topics regarding media locations:

- Placing Renditions Within Content Server
- Placing Renditions Outside Content Server
- Placing Renditions Within and Outside Content Server
- Setting Placement Location Configuration Variables
- Configuring Specific Media Format Placement Locations

24.4.3.1 Placing Renditions Within Content Server

Using the `weblayout` directory as the media location keeps assets within Content Server, but prevents assets from being accessed outside of Content Server. Assets stored outside Content Server can be sent to multiple locations with different access rights and different backup schedules, for example, or can be served from different media servers or web servers.

Setting Placement Location Configuration Variables details the procedure for setting configuration variables needed to specify media locations. Example 24-1 shows the configuration necessary for storing media renditions in the Content Server weblayout directory.

Example 24-1 Storing Media Renditions in the Content Server Weblayout Directory

Content Server Settings

No Content Server configuration variables need to be set when storing everything in the `weblayout` directory.

Inbound Refinery Settings

Set the following variable in the Inbound Refinery `UCM_server1_intradoc.cfg` file to point to the Content Server `weblayout` directory:

```
DefaultMediaPhysicalRoot-agentName=agentWeblayoutDir
```

where *agentName* is the IDC_Name of the Content Server and *agentWeblayoutDir* is the `weblayout` directory of Content Server, relative to the Inbound Refinery.

If Content Server is using partitions set up using File Store Provider, a configuration entry must be made for each partition. For example, if the Content Server has a partition defined as `damPartition` on root `$#env.WeblayoutDir$/damPartition/`, then the entry would be:

```
DefaultMediaPhysicalRoot-agentNameOnpartitionName=agentdamPartitionPath
```

where *agentName* is the IDC_Name of Content Server, *partitionName* is the name of the partition, and *agentdamPartitionPathName* is the path to the partition root, relative to Inbound Refinery.

24.4.3.2 Placing Renditions Outside Content Server

Placing assets outside of Content Server allows renditions to be accessed by other servers, such as a streaming media server or a web server. When placing assets outside of Content Server, the location of assets must be set in the configuration files of both Inbound Refinery and Content Server. A URL root must also be set in the configuration file for Content Server. The following example shows the configuration necessary for storing media renditions outside Content Server.

> **Note:**
>
> Both Content Server and Inbound Refinery must have physical access to the placement locations. To access any renditions outside of Content Server a separate web server must be installed and configured.

> **Note:**
>
> Make sure that the URL root `DefaultMediaUrlRoot` is specified in lowercase otherwise the assets may not work correctly.

Example 24-2 Storing Media Renditions Outside Content Server

Content Server Settings

The following configuration setting must be set in the Content Server `intradoc.cfg` file to specify the physical and URL roots of the media location:

```
DefaultMediaPhysicalRoot=\\\\mediaServer/ucmmedia/
DefaultMediaUrlRoot=http://mediaServer/media/
```

If Content Server is using partitions set up with File Store Provider, then each partition is a subdirectory of the root location set in `DefaultMediaPhysicalRoot`. By default, Content Server will store the media to the location specified in the DefaultMediaPhysicalRoot setting appended with the partition name.

For example, if `DefaultMediaPhysicalRoot=\\\\mediaServer/ucmmedia/` then media would be stored at:

```
\\\\mediaServer/ucmmedia/partitionName
```

Similarly, the default for the URL root set in `DefaultMediaUrlRoot` would be automatically appended with the partition name. For example, if `DefaultMediaUrlRoot=http://mediaServer/media/`, then the media would be accessed at:

```
http://mediaServer/media/partitionName
```

A File Store Provider partition can optionally be defined to be used as the physical and URL root by setting `DefaultMediaPhysicalRootOn`*partitionName* and `DefaultMediaUrlRootOn`*partitionName*. For example:

```
DefaultMediaPhysicalRootOnpartitionName=\\\\mediaServer2/ucmparition/
DefaultMediaUrlRootOnpartitionName=http://mediaServer2/ucmparition/
```

Inbound Refinery Settings

Set the following entry in the Inbound Refinery `intradoc.cfg` file:

```
DefaultMediaPhysicalRoot-agentName=\\\\mediaServer/ucmmedia/
```

where *agentName* is the IDC_Name of Content Server.

If `DefaultMediaPhysicalRootOn`*partitionName* was set in the Content Server `intradoc.cfg` file, then it must also be set in the Inbound Refinery `intradoc.cfg` file, so that both settings resolve to the same location:

```
DefaultMediaPhysicalRootOnpartitionName=\\\\mediaServer2/ucmparition/
```

24.4.3.3 Placing Renditions Within and Outside Content Server

In some situations it may be useful to use the `weblayout` directory as the media location for most renditions but place a particular format outside Content Server. For example, you may want a `.MOV` rendition stored within Content Server but have the `.WMV` and `.WMA` renditions placed outside Content Server for access by a streaming media server. The following example shows the configuration necessary for storing media renditions both inside and outside Content Server.

> **Note:**
>
> Both Content Server and Inbound Refinery must have physical access to the placement locations.

Example 24-3 Storing Media Renditions Inside and Outside Content Server

Content Server Settings

Follow the examples specified in the Content Server section of Example 24-2 to specify the physical and URL roots of the media.

Set the following variable to specify that the `.WMV` and `.WMA` files are to be treated differently from other renditions:

```
WinMediaSupportEnabled=true
```

Set the following variable in the Content Server `intradoc.cfg` file to specify where to locate the `.WMV` and `.WMA` files:

```
WinMediaPhysicalRoot=\\\\winmediaServer/ucmRenditions/windowsMedia/
WinMediaUrlRoot=rstp://winmediaServer/ucmRenditions/windowsMedia/
```

Inbound Refinery Settings

Follow the examples specified in the Inbound Refinery section of Example 24-2 to specify the physical root of the media.

Set the following variable in the Inbound Refinery `intradoc.cfg` file to specify that the `.WMV` and `.WMA` files are to be treated differently from other renditions:

```
WinMediaSupportEnabled=true
```

Use the following variable to specify what formats to place outside Content Server:

```
WinMediaFormats=wmv|wma
```

Set the following variable to specify the location for the `.WMV` and `.WMA` files:

```
WinMediaPhysicalRoot-agentName=\\\\winmediaServer/ucmRenditions/windowsMedia/
```

Procedures for setting locations for specific formats are detailed in Configuring Specific Media Format Placement Locations.

24.4.3.4 Setting Placement Location Configuration Variables

To set the asset placement locations:

1. Open the `intradoc.cfg` file in the connection directory *`DomainDir`*`/ucm/ibr/bin` for each Inbound Refinery connection accessing the shared directories in a standard text editor.
2. Add the `DefaultMediaPhysicalRoot` variable equal to the default location where video renditions will be placed. Because Inbound Refinery may be converting for several Content Servers, the agent name of the Content Server must be appended to the variable. For example:

   ```
   DefaultMediaPhysicalRoot-AgentName=\\\\NetworkIdentity/contentserver/weblayout/
   ```

   > **Note:**
   >
   > This is a root directory only. The media file will actually exist in a subdirectory that mirrors the typical Content Server `/weblayout/` directory. The path can be a local, mapped, or a Universal Naming Convention (UNC) path. The backslash is an escape character in Java, so any path using a backslash must be escaped using two backslashes.

3. Open the `intradoc.cfg` file in the connection directory *`DomainDir`*`/ucm/cs/bin` for each Content Server connection accessing the shared directories in a standard text editor.

> **Note:**
>
> Depending on network set-up, this path may or may not be identical to the path set in the Inbound Refinery `intradoc.cfg` file, but the two paths must resolve to the same location.

4. Add the `DefaultMediaPhysicalRoot` variable to each Content Server and set it equal to the default location video renditions are placed by the refinery server. For example:

   ```
   DefaultMediaPhysicalRoot=\\\\NetworkIdentity/contentserver/weblayout/
   ```

5. Set `DefaultMediaUrlRoot` equal to the default location of the URL root path, including the protocol, to where the file can be accessed. For example:

   ```
   DefaultMediaUrlRoot=http://NetworkIdentity/contentserver/
   ```

> **Note:**
>
> The `DefaultMediaPhysicalRoot` variables for each Content Server agent using Inbound Refinery must resolve to the same location as the respective `DefaultMediaPhysicalRoot-`*AgentName* variables for the refinery. Additionally, each `DefaultMediaUrlRoot` variable in Content Server must resolve to the same location as the Content Server `DefaultMediaPhysicalRoot` for that server.

6. Save changes and close the `intradoc.cfg` file.
7. Restart managed servers.

If all rendered video assets are to go to the set locations, then setting the variables in the configuration files are that is needed. To send some media formats to other locations (for example all `.ra` files to a streaming server or all `.mpg` files to an external storage system), then the locations for those formats must also be configured.

24.4.3.5 Configuring Specific Media Format Placement Locations

Different locations can be specified for differing video renditions based on the media format. Media categories are available to define physical and URL roots for different formats:

- WinMedia
- DarwinMedia
- HelixMedia
- QuickTimeMedia
- RealMedia

These category names serve as labels only, and any format can be grouped under any category label.

In order to specify different locations for different formats, edit the `intradoc.cfg` files for both Inbound Refinery and Content Server to:

- enable a category
- specify the formats handled by the category
- set the physical root specific to the category

For Content Server only:

- set the URL root specific to the category

> **Note:**
>
> Both Content Server and Inbound Refinery must have physical access to the placement locations.

To set a different location for a specific format:

1. Open the *DomainDir*`/ucm/ibr/bin/intradoc.cfg` file for each Inbound Refinery connection accessing the shared directories in a standard text editor.
2. Enable a category by setting the appropriate variable equal to true. For example, the following variable may be set:

   ```
   WinMediaSupportEnabled=true
   DarwinMediaSupportEnabled=true
   HelixMediaSupportEnabled=true
   ```

3. Set the format of the media handled by the category by setting the appropriate variable equal to the format extension. For example:

   ```
   WinMediaFormats=wm*|asf|asx
   ```

   Each format is separated by a pipe (|) and an asterisk (*) can be used as a wildcard.

   The following variables may be set, and must match the enabled category or categories:

   - `WinMediaFormats`
   - `DarwinMediaServerFormats`
   - `HelixMediaServerFormats`

4. Set the physical root for the media handled by the category by setting the appropriate variable equal to the physical path. For example:

   ```
   HelixMediaPhysicalRoot=\\\\NetworkIdentity/RealMedia/
   ```

   The following variables may be set, and must match the enabled category or categories:

   - `WinMediaPhysicalRoot`
   - `DarwinMediaPhysicalRoot`
   - `HelixMediaPhysicalRoot`

> **Note:**
>
> This is a root directory only. The media file will actually exist in a subdirectory that mirrors the typical Content Server `/weblayout` directory. The path can be a local, mapped, or a Universal Naming Convention (UNC) path. The backslash is an escape character in Java, so any path using a backslash must be escaped using two backslashes.

5. Open the *`DomainDir`*`/ucm/cs/bin/intradoc.cfg` file for each Content Server connection accessing the shared directories in a standard text editor.
6. Repeat steps 2 through 4 in the Content Server `intradoc.cfg` file.
7. In the Content Server `intradoc.cfg` file, add one of the following variables based on the formats being rendered, and set it to the URL root path, including the protocol, where the file can be accessed. For example:

   ```
   HelixMediaUrlRoot=rtsp://NetworkIdentity:554/
   ```

   The following variables may be set, and must match the enabled category or categories:

   - `WinMediaUrlRoot`
   - `DarwinMediaUrlRoot`
   - `HelixMediaUrlRoot`
8. Save changes and close the `intradoc.cfg` file.
9. Restart managed servers.

24.4.4 Using Streaming Servers

Depending on how media conversions are set, categories, and URL root variables, renditions can be served out of a web server or streaming media server. The following actions must be performed to stream rendered videos:

- install and properly configure a supported media server based on the instructions that came with the media server
- set the conversion application to deliver the correct streaming format
- configure a category to deliver the rendition to the correct place
- configure the web URL root with the proper protocol and syntax for the streaming server

Digital Asset Manager supports Darwin Streaming Server (QuickTime), Helix Streaming Server (RealMedia), and Windows Media Server. For information about protocols used with streaming media, see the media server documentation.

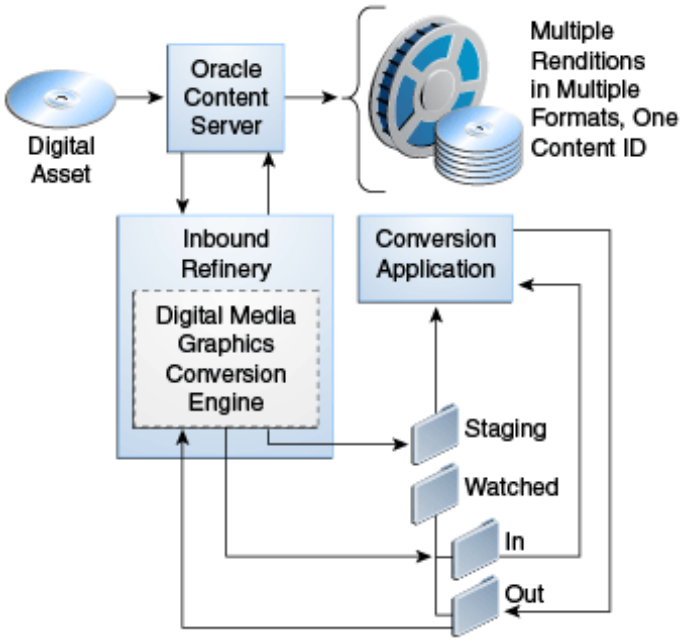
24.4.5 Defining Video Rendition Sets

When a file is checked into Content Server, the format of the file determines if it is a digital asset. If it is a video file, Content Server passes the file to Inbound Refinery, which notifies the video conversion application a file is there to convert. The resulting renditions are then passed back through Inbound Refinery to Content Server or other

specified locations, where they are managed under a single content ID and made available to the organization.

See Setting Up and Managing Video Conversions for more information about video renditions. See the Downloading Specific Video Renditions in WebCenter Content blog for information about downloading video renditions.

Figure 24-1 Rendering a Video Asset



24.4.6 Importing the WindowsMediaWorkflow.xml File

After installing Vantage, it is recommended that you import the WindowsMediaWorkflow.xml file located in the `IdcHomeDir/components/DAMConverter/Vantage` folder. This workflow creates all the variables, labels and style sheets required by the Digital Asset Manager integration.

To import the workflow:

1. Start the Vantage Workflow Designer.
2. Go to File, Import Workflows...
3. Select or create a category for the workflow.
4. Verify that the paths on the initial Watch Action and the final two Deploy Actions are valid in your environment.
5. Activate the workflow.

This workflow produces up to three renditions:

- A Windows Media (wmv) rendition of the input
- A set of keyframes for the storyboard
- If the input has closed captions, a W3C TTML file is produced.

24.4.7 Understanding the Vantage Workflow

This section describes the main steps in the Vantage workflow for Digital Asset Manager. Each Digital Asset Manager video rendition set must be created with a separate Vantage workflow.

Each workflow starts with a Watch action. The Watch action is configured to watch the “in” directory for each rendition. After the Watch action picks up the job, the workflow splits into multiple parts. In this section, we’ll discuss the workflow for media files with both audio and video streams.

Producing the video rendition

The following is an overview of this process:

1. A Flip action creates every rendition in the rendition set. Each Flip action must set the Vantage variable "Rendition Name." This variable is the WebCenter Content Digital Asset Manager Rendition name in the WebCenter Content user interface.

   To set the Vantage variable “Rendition name”:

   a. Right-click the action and select **Add Variables...** .

   b. In the Add Variable dialog, add the "Rendition Name" variable.

2. Each Flip action that produces video renditions has two Identify actions; these actions identify properties about the rendition. In one Identify action the attributes for the following variables are identified:

Variable	Description
Movie Duration	Identifies the content duration
Video Width	Identifies the video width
Video Height	Identifies the video height
Video Framerate	Identifies the video frame rate
Video Bitrate	Identifies the video bit rate

3. The second Identify action identifies the following variable:

Variable	Description
File name	Identifies the file name

4. The Identify Actions feeds a Populate action. The Populate action populates variables identified by the Identify action into the WebCenter Content Digital Asset Manager Renditions Metadata Label. The WebCenter Content Digital Asset Manager Renditions Metadata Label has the following fields:

Field	Description
RenditionName	Populated by the Vantage variable “Rendition Name”. Both video rendition and Keyframes renditions use this for identification.
FileName	Populated by the Vantage variable “File Name”. Used by video renditions.

Field	Description
Bitrate	Populated by the Vantage variable “Bitrate”. Used by video renditions.
Duration	Populated by the Vantage variable “Duration”. Used by video renditions.
Framerate	Populated by the Vantage variable “Framerate”. Used by video renditions.
Height	Populated by the Vantage variable “Height”. Used by video renditions.
Width	Populated by the Vantage variable “Width”. Used by video renditions.
CaptureInterval	Populated by the Vantage variable “Capture Interval”. Used by Keyframe renditions.

5. The label created by the Populate action feeds a Transform action to transform the WebCenter Content Digital Asset Manager Renditions Metadata Label into the WebCenter Content Digital Asset Manager Style Sheet. Inbound Refinery reads this XML attachment to get information for each video rendition of the set.
6. All Transform and/or Examine actions feed a Deploy action that copies the rendition and files created by the workflow to the "out" directory for the rendition set.
7. After the Deploy action, a Delete action deletes the original file from the "in" directory. When the workflow deletes the original file, Inbound Refinery knows the workflow is complete.

> **Note:**
>
> Ensure that the Delete action is set to execute regardless of the state: Right-click and select **Perform On**, then **Any**. This ensures the original file gets deleted even if the workflow has an error. In case of a workflow error, check Vantage for error message details.

> **Note:**
>
> Every time Inbound Refinery finishes a workflow, it checks the "in" and "out" directories for old files and deletes them. By default any file more that 1 day old is deleted. This can be changed by setting the “WatchedWorkflowOldJobCleanup" variable. This variable accepts an integer value and one of the following suffixes: "year", "month", "week", "day", "hour", "minute", "second". For example, if you want files to be considered old after 3 hours, set WatchedWorkflowOldJobCleanup to 3hour.

Producing the optional storyboard

The following is an overview of this process:

1. A Flip: JPEG Keyframe action is needed to produce the storyboard. This Flip action sets the following variables:

Variable	Description
Rendition Name	Set to Keyframes.
KeyFrameInterval	Set to the interval to capture the image. For example, if the storyboard on the user interface should have an image every 5 seconds, set this variable to 00:00:05:00 29.97 fps.
Configure JPEG Setting	Capture Mode must be set to "Repeating Keyframes" and the Capture Interval must be bound to the "KeyFrameInterval" variable.

2. The Flip: JPEG Keyframe feeds a Populate action. The Populate action populates variables identified by the previous action into the WebCenter Content Digital Asset Manager Renditions Metadata Label. Note that not all the variable in the label are used.
3. The label created by the Populate action feeds a Transform action to transform the WebCenter Content Digital Asset Manager Renditions Metadata Label into the WebCenter Content Digital Asset Manager Style Sheet. Inbound Refinery reads this XML attachment to get information about the story board for the rendition set.

Producing the optional closed captions

If the rendition set is expected to produce text from the closed captions, an Examine action is required following the Watch action. An Examine: Examine media video and audio action produces a W3C TTML attachment that is deployed by the Deploy action.

24.4.8 Managing Video Conversion

Content Server identifies content items as digital assets based on the extension of the file checked in. At installation, Digital Asset Manager checks to see if the file formats exist in the Content Server Configuration Manager applet.

This section discusses the following topics:

- Editing the Video File Type Configuration Table
- Setting the Default Video Format Preferences

24.4.8.1 Editing the Video File Type Configuration Table

If you add a file format and map the extension to the Digital Media Video conversion engine, and need that format to play in an embedded player (such as on the Rendition Information page), the extension must exist in the Video File Type configuration table of the *IdcHomeDir*`/components/DAMConverter/resources/dam_cfg_tables.htm` file.

The format must exist in the Video File Type configuration table only for the file to play in an embedded player. If the format is not in the table, the rendition can still be opened and played in a standalone player that supports the rendered format.

To verify that the added format exists in the Video File Type configuration table, open the `dam_cfg_tables.htm` file in a standard browser and review the file extensions listed. If the file extension does not exist, write a custom component listing the extension and additional necessary information and merge the tables. For more information about creating custom components, see *Developing with Oracle WebCenter Content*.

<@table VideoFileTypes@>

fileExtension	formatName	player	metafileExtension
rm	Real	real	ram
ra	Real	real	ram
wmv	WindowsMedia	wmplayer	asx

The following table lists the columns of the Video File Type configuration table and their function.

Column Name	Definition
fileExtension	The extension of the file formats to be supported played in the embedded players.
formatName	The name of the format associated with the extension. This value corresponds to the values in the Video Format Prefs table, which is configurable, and is displayed in the choice lists of the embedded players.
player	The player that supports the added format extension. The values are case-sensitive. Currently only three values are allowable: • real • quicktime • wmplayer
metafileExtension	The metafile extension associated with the format extension, used to determine what embedded player will play a streaming version of the format. There must be a value in this field if the format is streamed.

24.4.8.2 Setting the Default Video Format Preferences

Embedded players are displayed on the Rendition Information page or when a web-viewable link is clicked. The format chosen to play in the embedded player is based on a table of user preferences regarding available rendition format options, set on the Video Preferences page. Prior to user input, default preferences are based on values set in the Video Format Preferences table of the *IdcHomeDir*`/components/DigitalAssetManager/dam_cfg_tables.htm` file.

`IdcHomeDir/components/DigitalAssetManager/`

<@table VideoFormatPrefs@>

format	pickOrder_win	pickOrder_mac	pickOrder_other
Real	3	3	3
WindowsMedia	1	4	4
Quicktime	4	1	2
MPEG	2	2	1

<@end@>

To add new settings or modify default preferences, create a custom component containing the new or modified settings and merge the custom data table into the corresponding default data table. For more information about creating custom components, see *Developing with Oracle WebCenter Content*.

> **Note:**
>
> Do not edit a standard Content Server component resource directly. Always create a custom component to merge changes into Content Server or Inbound Refinery.

Modifications made to a component resource are overwritten if Digital Asset Manager is updated to a newer version.

The following table lists the columns of the Video Format Preferences table and their function:

Column Name	Definition
format	Configurable name displayed in the choice list of an embedded player.
pickOrder_win	Determines the order a format is selected on a Windows operating system.
pickOrder_mac	Determines the order a format is selected on a Macintosh operating system.
pickOrder_other	Determines the order a format is selected on an operating system other than Windows or Macintosh.

24.4.9 Using the Command-Line Interface (CLI) Tool for Video Rendition Sets

Starting with the 12c release, Digital Asset Manager allows the use of command-line interface (CLI) tools to produce video rendition sets.

To produce video rendition sets, define the video renditions in the file *IntradocDir*/data/configuration/dam/extraRendition_definitions.hda just like image renditions. For more information, see Creating and Configuring Image Rendition Sets.

This section contains the following topics:

- Creating Video Renditions with CLI Tool
- Gathering Video Metadata Using CLI Tool

24.4.9.1 Creating Video Renditions with CLI Tool

To produce video rendition sets, define the video renditions in the file *IntradocDir*/data/configuration/dam/extraRendition_definitions.hda just like image renditions.

1. In the LocalData section defined the paths to the CLI tools used to create the video rendition.

2. Define a ResultSet for the video rendition set. ResultSets are used to define the rules used to create the video rendition. These ResultSets have six fields. See Adding a Rendition Set for more information on the rendition ResultSet structure.

Field	Use
extRenditionName	The rendition name. The name listed in the Content Server metadata field *xVideoRenditions*.
extEngine	An IdocScript expression that evaluates to a path to an executable. The variables are usually defined in the LocalData section of the extraRendition_definitions.hda file.
extType	The type of rendition to be made in the form: [video|keyframes]|<parameters for the rendition>.
extSourceFile	The source (or input) file for this rendition, usually the IdocScript variable <$InFilePath$>.
extParameters	The string of parameters used to create the rendition, this column is IdocScript enabled. This column can be used in two ways: • hard-code parameters in this column • set a variable in the LocalData to a string parameters and use the variable repeatedly in several renditions
extDescription	The name of the rendition in WebCenter Content. This field is used only with video renditions, otherwise leave it blank.

The **extType** column in the rendition ResultSet is used to tell Inbound Refinery how to collect the results from the CLI tool. Currently, with a CLI tool, only video renditions and a set of keyframe renditions can be created.

Each video rendition set must have at least one video rendition, and no more than one keyframe rendition.

Video Renditions
For video rendition the **extType** must start with *video* and include the *outputExtension* parameter. The following will create a video rendition with a wvm extension:

```
video|outputExtension=wmv
```

Keyframe Renditions
For video rendition the **extType** must start with *keyframe* and include the parameters: *outputExtension* and *frameIntervalSeconds*.

- The *outputExtension* is the file extension of the keyframe image files
- The *frameIntervalSeconds* is the number of seconds between keyframe images

3. Add the name of the ResultSet to the Content Server metadata field *xVideoRenditions* so that it can be selected/assigned at check-in of the video.

The following is an example extraRendition_definitions.hda that defines a WMV rendition set that uses FFmpeg to create a Windows Media rendition and a set of keyframes that are 4 seconds apart:

```
@Properties LocalData
FFMpegPath=/path/ffmpeg.exe
@end

@ResultSet WMV
6
extRenditionName
```

```
extEngine
extType
extSourceFile
extParameters
extDescription
WinMedia
<$FFMpegPath$>
video|outputExtension=wmv
<$InFilePath$>
-i "<$inFile$>" "<$outFile$>.wmv"
Windows Media
StoryBoard
<$FFMpegPath$>
keyframes|frameIntervalSeconds=4,outputExtension=png
<$InFilePath$>
-i "<$inFile$>" -vsync 1 -r 0.25 -s 320x240 -f image2
"<$outDir$>\keyframe%03d.png"
unused description
@end
```

24.4.9.2 Gathering Video Metadata Using CLI Tool

You can get the video properties of each video rendition using the command-line interface (CLI) tool. This ensures that Inbound Refinery and Digital Asset Manager return all the data about a video rendition that the Content Server user interface expects to display.

To get the video properties of a video rendition:

- Set the following keys in the LocalData section of the extraRendition_definitions.hda file.

LocalData Key Name	Description
MediaRenditionInfoPath	The path to the command-line interface tool
MediaRenditionInfoParameters	The parameters used by the command-line interface tool
MediaRenditionInfoNodeMap	An additional table defined in the extraRendition_definitions.hda file that maps the xml output of the CLI to the expected keys. This table has the following fields: • mediaInfoKey: The expected key Digital Asset Manager needs. It includes the following rows: Bitrate, Duration, Framerate, Height, and Width • mediaXmlNodeName: The node in the CLI output for the expected field. If the xml has duplicate nodes, Inbound Refinery uses data from the first node.

The following is an example extraRendition_definitions.had file:

```
@Properties LocalData
MediaRenditionInfoPath=D:/3rdParty-Bin/
MediaInfo_CLI_0.7.67_Windows_i386/MediaInfo.exe
```

```
MediaRenditionInfoParameters=--Output=XML -f <$mediaPath$>
MediaRenditionInfoNodeMap=MediaInfoNodeMap
@end

@ResultSet MediaInfoNodeMap
2
mediaInfoKey
mediaXmlNodeName
bitrate
Bit_rate
duration
Duration
framerate
Frame_rate
height
Height
width
Width
@end
```

25
Managing PDF Watermark

A watermark is a image or text superimposed on selected pages in a PDF document. When enabled, the PDF Watermark component can apply a watermark at check-in (static watermark) or when a user requests to view or download a PDF document (dynamic watermark).
PDF Watermark can also add security features to PDF files as they are downloaded for viewing. Password security can be added, and the ability to print or copy the contents of the file can be enabled or disabled.

This chapter provides information about managing PDF Watermark:

- Understanding PDF Watermark
- Configuring PDF Watermark
- Watermarking Scenarios

25.1 Understanding PDF Watermark

This section discusses the following topics:

- Types of Watermark
- Templates
- Dynamic Watermark Rules
- PDF Optimization
- Watermark Placement

25.1.1 Types of Watermark

A static watermark is applied during content check-in as a follow-on step to the Inbound Refinery conversion. To select a watermark for content to be converted to PDF, enter a valid **Watermark Template ID** during check in. Only documents that Inbound Refinery converts to PDF can receive a static watermark. After a document receives a static watermark, all viewers of the document see the same watermark.

In the same way, content checked in by an automated process such as WebDAV or BatchLoader can also be given a static watermark, provided a valid Watermark Template ID is provided. For more information about creating templates and template IDs, see Templates.

Dynamic watermarks are generated as needed when a user requests to view or download a PDF document. Dynamic watermarks can contain variable information (for example, the user name or the requesting user, or the date and time of download). For this reason, different users may see the same content with different watermarks. With dynamic watermarks, only the web layout form is watermarked. The original PDF file is unchanged in its vault location.

Dynamic watermarking is rules-based. If a request for a PDF document satisfies a pre-defined rule, the template associated with that rule is used to watermark a copy of the content

before the copy is returned to the requesting user. System administrators define rules and set up specific conditions for determining which requested content gets a dynamic watermark.

For more information about specifying rules for dynamic watermarks, see Dynamic Watermark Rules.

The following kinds of watermarks can be used:

- **Text:** Specified the text which can include metadata values for the content item, and include special keywords, such as $DATE$, that provide information about the content item at the point it is watermarked.
- **Image:** An image in any of the supported bitmap (raster) formats.
- **Signature:** If Electronic Signatures is enabled, a watermark can be created from the electronic signature metadata associated with a content item.

Details are specified for type of watermark as well as placement. One or more watermarks of any type can be used in a given document. Defined watermarks are stored in a template that is checked in with a content ID and default metadata values.

25.1.2 Templates

Whether a watermark is applied statically at check-in or dynamically when the PDF file is requested, the watermark information is stored in a template which includes information about the text or image watermark itself and any rules defined for its use.

Legacy schema templates are supported for watermarking, but any change to the template results in an upgrade to the new schema. Consequently, any template which is changed in Content Server version 12*c* may not work correctly with older versions of Content Server.

For information about creating templates, see Adding or Editing Templates.

A template is checked into the content repository as a managed content item with default metadata and two additional metadata fields:

- **Watermark Template ID:** The content ID (dDocName) for the template which can be assigned when the template is created. This is specified for static watermarks when the content item is checked in.
- **Watermark Template Type:** A list of supported template types. Currently, a single option is provided, the default PDFW_Template.

In addition to these fields, additional metadata values can be specified. This helps ensure that default values are provided for fields that require a value.

25.1.2.1 Template Security

A user password requires the user to provide a password to open and view the PDF. An owner password restricts the ability to change the PDF file or modify the security settings within the PDF file.

These security settings set access restrictions within the associated PDF file itself using PDF security. These access restrictions are independent of access restrictions to the content item defined by Content Server.

User/Owner passwords are encrypted in the PDF Watermark Template with a third-party encryption library. Encryption is performed automatically when the template is

saved and decryption is performed automatically when the template is used for a watermark.

Oracle does not provide an encryption library. The library `bcprov-jdk14-138.jar` is a recommended third-party encryption library that is downloadable from BouncyCastle.org, but any library can be used. For information about specifying an encryption library, see Specifying the Classpath for an Encryption Library.

Passwords in legacy templates are not encrypted until the template is saved. A template cannot be saved unless it is changed. Therefore, to encrypt template passwords, edit each legacy template and make a minor change before saving.

25.1.3 Dynamic Watermark Rules

Rules are used to determine which template is applied for dynamic watermarking. After creating a template, the rules for the template can be defined. The same template can be used for static or dynamic watermarking. Rules are used only for dynamic watermarking.

If a template has multiple rules, the rules are applied in the order listed. Rules should be ordered with the most specific tests earlier in the list, and more general ones after that. All rules must test positive for the watermark to be applied.

Within a rule, criteria can be set based on the values of selected metadata fields. For example, you can test the `dDocAuthor` field for specific authors or the `dDocType` for a specific type of document. The order in which you define criteria for a rule does not matter. All criteria must be true for the associated rule to test positive.

25.1.4 PDF Optimization

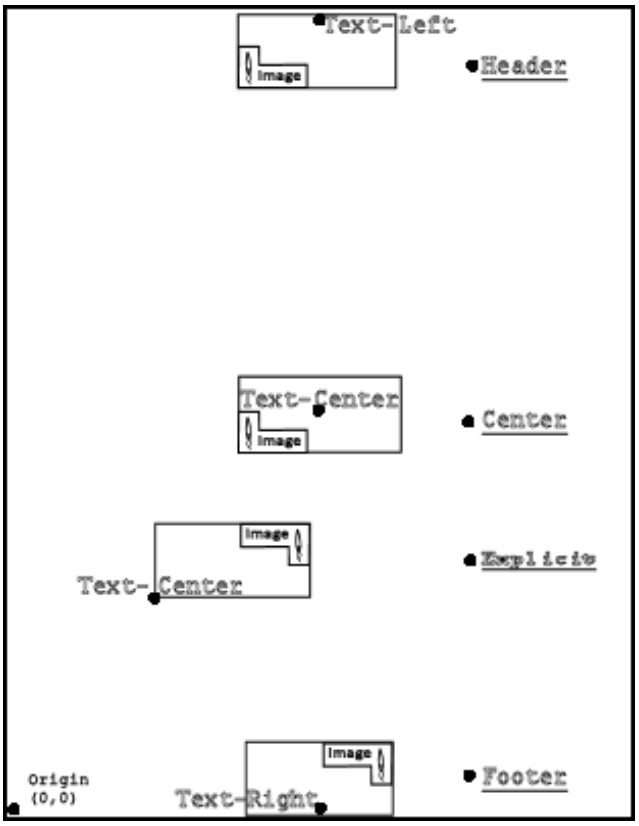
PDFs that come from the PDF Converter may have been optimized for faster Web viewing. If a static watermark is applied to that content, the optimization is lost. Post-watermarking optimization requires a third-party optimizer which is not provided with PDF Watermark. To use optimization, a distiller engine/optimizer must be installed and fully operational. The chosen optimizer must be able to execute conversions with a command-line (for example, a script file or a `.bat` file).

> **Note:**
>
> A PDF optimizer is not provided with PDF Watermark. If using the Optimization feature, install a third-party distiller engine before use and verify it is fully operational. The optimizer must be able to execute conversions on a command-line (for example, a script file or a `.bat` file).

25.1.5 Watermark Placement

Options are available for placing text or image watermarks at the top (header), center, or bottom (footer) of the page or at a particular location on the page with X-Y coordinates. Multiple watermarks can be used on a given document.

In the image below, the reference points for each of the positions is indicated by a point. The example image in each of the positions shows the orientation relative to the associated reference point. Example text in each of the positions shows one of the available horizontal alignment options (left, right, center). All text alignment options are available at each of the positions.



For standard placement, text and images reference a point at the top-center, middle-center, or bottom-center of the page. Images center horizontally around the associated reference point. With text, you can specify the horizontal alignment of the text with respect to this reference point (left, right, or center aligned).

For explicitly placed watermarks, the coordinates are in *points*, with each point equal to 1/72". The origin (0, 0) is the lower left corner of the page. For images, these coordinates specify the lower left corner of the image with the image extending up and to the right. For text, these coordinates specify the horizontal reference point for the alignment options, similar to the standard placement options.

25.2 Configuring PDF Watermark

This section describes tasks that are used to manage PDF Watermark.

- Specifying the Classpath for an Encryption Library
- Starting PDF Watermark Administration
- Adding or Editing Templates
- Creating and Editing Rules

25.2.1 Specifying the Classpath for an Encryption Library

The passwords defined in a template set corresponding passwords within the PDF file itself when the PDF file is rendered. The passwords stored in the template are encrypted using a third-party encryption library. A reference to an encryption library

used with PDF Watermark must be provided for the Content Server to encrypt passwords stored in the template.

Oracle does not provide an encryption library for encrypting passwords. This procedure assumes the use of a third-party encryption library. One such library is the Bouncy Castle Crypto APIs for Java which is downloadable from BouncyCastle.org, but any library can be used. Use a version that matches the JDK version on your machine.

1. Download an encryption library `.jar` file and save it to a location that the Content Server can access.
2. launch the System Properties application. For more information, see Running Administration Applications in Standalone Mode.
3. On the Systems Properties applet, open the **Paths** tab.
4. Specify the path to the encryption library jar file from step 1.
5. Click **OK** to save the changes and exit the System Properties utility.

25.2.2 Starting PDF Watermark Administration

Templates, rules and configuration for PDF Watermark are managed in using the PDF Watermark Administration page.

1. From the main menu, choose **Administration** then **PDF Watermark Administration**.
2. Click **PDF Watermark Administration**.

   The PDF Watermark Administration page opens.

25.2.3 Adding or Editing Templates

Define any required metadata field values before creating a template. After checking in the template, it can be modified as needed.

25.2.3.1 Defining Metadata Fields

To define specific metadata fields for template check in:

1. From the main menu, choose **Administration** then **PDF Watermark Administration**.
2. On the PDF Watermark Administration page, click the **Configuration** tab.
3. Highlight the Field Name and Value pair to define/edit and click **Edit**.
4. On the Edit Default Value page, set the value to be applied for the Field name selected.
5. Click **Apply**.

25.2.3.2 Adding a Template

To add a template:

1. On the PDF Watermark Administration page, select the **Templates** tab.
2. To edit an existing template, select the template and click **Edit**. To create a new template, click **Add.**
3. On the Add New/Edit Template page, name the template and assign it a meaningful content ID. The ID cannot be changed after the template is checked in.

4. To add security to the template, click the **Security** tab.
    a. Select an encryption bit-depth for **Security Level**. The higher the number, the stronger the encryption. This encryption level applies to the passwords defined in the PDF file itself, not the watermark template. Oracle does not provide an encryption library for encrypting passwords stored in the template. For more information about adding an encryption library, see Specifying the Classpath for an Encryption Library.
    b. To restrict access to the PDF file associated with the template, specify a **User Password**. Users are required to specify this password to view or download the PDF.
    c. To restrict the ability to change the PDF file or modify the security settings within the PDF file, specify an **Owner Password**.

       This password applies to the associated PDF file itself, not the current watermark template. Access to the template is governed by Content Server's security model.
    d. To prevent the user from printing any portion of the PDF file, set **Print Allow** to **No**. To permit printing at low resolution, selected **Degraded**.
    e. To prevent the user from copying portions of the PDF file, set **Copy Allow** to **No**.
5. Click **OK** when done.

25.2.3.3 Add or Edit a Text Watermark

To add or edit a text watermark:

1. Open the Add New/Edit Template page and click the **Text Watermark** tab.
2. To add a watermark, click **Add**. To edit an existing watermark, click **Edit**. The
3. On the Add New/Edit Text Watermark page, specify the **Text** to appear in the watermark. The text can include embedded symbols that are replaced by document information, such as the page count or the document name when the watermark is rendered.
4. Select the **Location** on the page where the watermark appears.
5. If **Explicit** is selected, specify the **X-Coordinate** and **Y-Coordinate** location for the watermark. Values are specified in points. Each point is 1/72 in. measured from the lower-left corner of the page.
6. Specify the **Rotation** of text from 0 to 359 degrees, rotated counter clockwise.
7. Select the horizontal **Alignment** at the specified location.
8. Select the font, size, weight and color. Weight is disabled for those fonts that do not have an extended weight.
9. Select whether to **Layer** the watermark Over or Under the content in the PDF (including other watermarks).
10. Specify a **Page Range**. If left blank, the page range includes the entire document.

    Separate specific pages with commas (1,2,4). Separate the first and last pages in a page range with a colon (12:24). Use the keyword LAST to designate the last page without having to specify the actual page number. For example: 1,2,4,12:24,50:LAST.

11. Specify a Page Range **Modifier** to watermark **Even Pages Only** or **Odd Pages Only**.
12. Click **OK** when done.

25.2.3.4 Add or Edit an Image Watermark

Images must be checked in before use. To add or edit an image watermark:

1. Open the Add New/Edit Template page and click the **Image Watermark** tab.
2. To add a watermark, click **Add**. To edit an existing watermark, click **Edit**.
3. On the Add New/Edit Image Watermark page, specify the **Content ID** of the image to use. The image can be any supported bitmap (raster) image format, such as GIF or JPG.
4. Optionally specify a **Scale Factor** to preserve or modify the size of the image when it is used as a watermark. Without specifying a scale factor, images are rendered at 72 dpi.

   The Scale Factor is expressed as a percentage based on the following formula: *default_dpi /image_dpi* *100%. For example, to maintain the size and resolution of a 300 dpi image, you calculate the Scale Factor as follows: 72 dpi /300 dpi *100% =24% for a Scale Factor of 24.
5. Select the **Location** on the page where the watermark appears.
6. If **Explicit** is used for the location, specify the **X-Coordinate** and **Y-Coordinate** location for the watermark. Values are specified in points. Each point is 1/72 in. measured from the lower-left corner of the page.
7. Select whether to **Layer** the watermark Over or Under the content in the PDF (including other watermarks).
8. Specify a **Page Range**. If left blank, the page range includes the entire document.

   Separate specific pages with commas (1,2,4). Separate the first and last pages in a page range with a colon (12:24). Use the keyword LAST to designate the last page without having to specify the actual page number. The following page range includes all of these options: 1,2,4,12:24,50:LAST.
9. Specify a Page Range **Modifier** to watermark **Even Pages Only** or **Odd Pages Only**.
10. Click **OK** when done.

25.2.3.5 Add or Edit an Electronic Signature Watermark

To add or edit an electronic signature watermark:

1. Open the Add New/Edit Template page and click the **Signature Watermark** tab.
2. To add a watermark, click **Add**. To edit an existing watermark, click **Edit**.
3. On the Add New/Edit Signature Watermark page, specify the **Label** to appear in the watermark. The text can include embedded symbols that are replaced by document information, such as the page count or the document name when the watermark is rendered.
4. Specify the **Fields** to use in the watermark as a comma-delimited list. The fields are the user-defined fields from the Electronic Signatures table.
5. Select the **Location** on the page where the watermark appears.
6. If **Explicit** is used for the location, specify the **X-Coordinate** and **Y-Coordinate** location for the watermark. Values are specified in points. Each point is 1/72 in. measured from the lower-left corner of the page.

7. Select the font, size, weight and color. Weight is disabled for those fonts that do not have an extended weight.
8. Select whether to **Layer** the watermark Over or Under the content in the PDF (including other watermarks).
9. Specify a **Page Range**. If left blank, the page range includes the entire document.

   Separate specific pages with commas (1,2,4). Separate the first and last pages in a page range with a colon (12:24). Use the keyword LAST to designate the last page without having to specify the actual page number. For example: 1,2,4,12:24,50:LAST.
10. Specify a Page Range **Modifier** to watermark **Even Pages Only** or **Odd Pages Only**.
11. Click **OK** when done.

25.2.4 Creating and Editing Rules

A template must be created before rules can be defined. For more information, see Adding or Editing Templates.

To add or edit a rule:

1. On the PDF Watermark Administration page, select the **Rules** tab.
2. To add a new rule, click **Add.** To change an existing rule, select a rule and click **Edit.**
3. For a new rule, on the Add New/Edit Rule page, enter a **Name** that describes the way a rule is used. The name cannot be changed after saving. To change the name of a rule, delete the rule and create a new one.
4. Select a **Template ID** to associate with the rule.
5. To add a new criterion, click **Add**. To change an existing criterion, select the criterion and click **Edit**.
6. For a new criterion, on the Add New/Edit Criteria page, select the **Field Name.** After saving, the field selection cannot be modified. To specify a different field name, create a new criterion.
7. Specify the **Value** for the selected field. If the field chosen is a list, select a value from the options list.

> **Note:**
>
> Rules criteria are case-sensitive. The value must match the case of the returned value. For example, if the title you enter is "foobar" and the value returned is "FooBar", it is considered a mismatch and the rule fails.

8. To save the criterion, click **OK**.
9. To save the criteria for the current rule, click **OK**.

   Within a rule, the order of criteria does not matter. All criteria must be satisfied for the rule to apply.

10. To change the order of the rules assigned to the template, select a rule and use the **Move Up** and **Move Down** buttons to change the position of the rule in the list.

    The order in which the rules are tested can be significant, depending on the criteria used. In general, order the rules with the most specific tests (number of criteria) high in the list, and the more general ones (fewer criteria) lower down.

11. Click **OK**.

25.3 Watermarking Scenarios

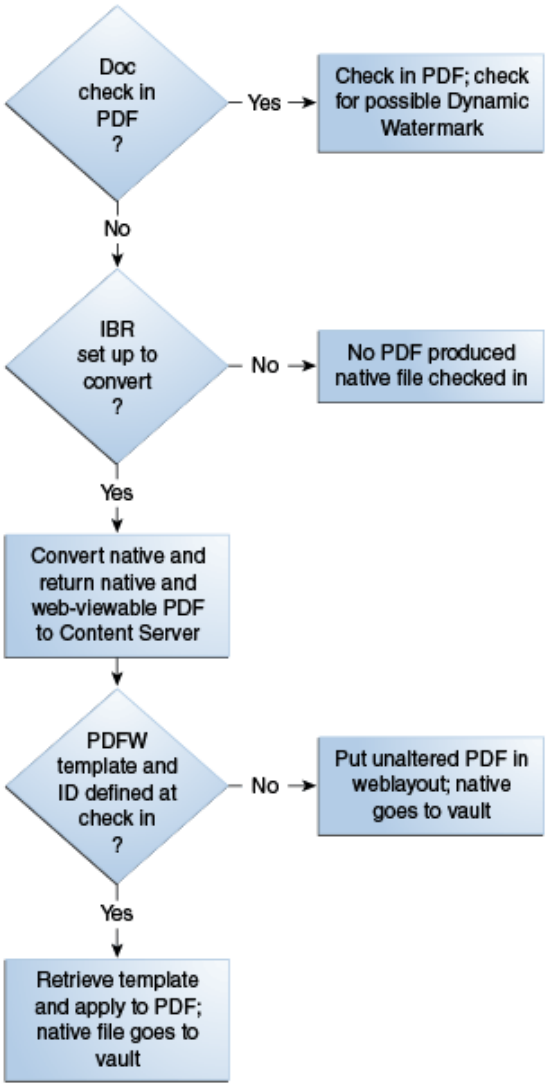
This section discusses the following topics:

- Static Watermarking Scenario
- Dynamic Watermarking Scenario

25.3.1 Static Watermarking Scenario

Content Server receives processed content from Inbound Refinery. Inbound Refinery must have PDF Converter installed, enabled, and configured to convert the necessary file formats into PDF. When the PDF file is presented, the watermark template selected during the content check in is applied.

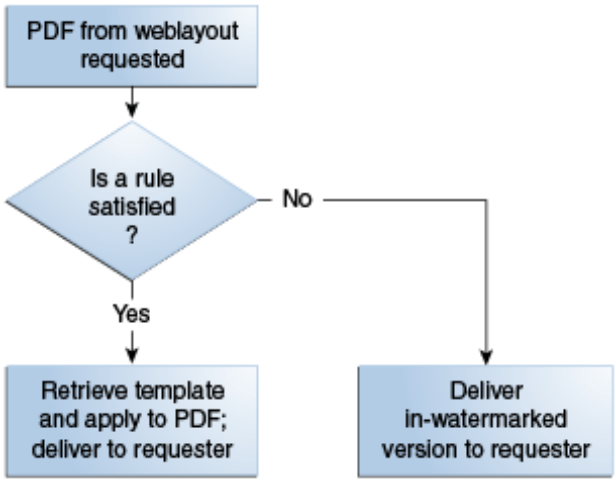
Watermark elements are pre-defined in the template used to watermark the incoming PDF. The watermark is applied and is delivered to requesters without regard for dynamic watermarking rules. Rules-based watermarking (Dynamic) can also be applied in addition to a static watermark.



25.3.2 Dynamic Watermarking Scenario

When a Web-viewable PDF is requested by a user, a check is performed based on the defined rulesets to determine if a watermark is applied to the Web-viewable PDF delivered to the requester.

If a request for a PDF document satisfies a pre-defined rule, the template associated with that rule is used to watermark a copy of the content before the copy is returned to the requesting user.



Note:

A PDF optimizer is not provided with PDF Watermark. If using the Optimization feature, install a third-party distiller engine before use and verify the optimizer is fully operational. The optimizer must be able to execute conversions on a command-line (for example, a script file or a `.bat` file).

26
Supported File Formats

Digital Asset Manager and Conversion products support a variety of file formats and conversion options, based on the type of file being converted and the method used for the conversion.

This section discusses these topics:

26.1 File Formats Converted by Outside In Technology

Outside In Technology is used by Inbound Refinery, PDF Export, and XML Converter.

26.1.1 Inbound Refinery

Inbound Refinery includes Outside In Image Export, which can be used for the following:

- To create thumbnails of files. Thumbnails are small preview images of content.
- To convert files to multi-page TIFF files, enabling users to view the files through standard web browsers with a TIFF viewer plugin.

26.1.2 PDF Conversion

PDF conversion includes Outside In, which can be used with WinNativeConverter on Windows to create PDF files of some content items. Using the native application, Outside In is used to print the files to PostScript, and then the PostScript files are converted to PDF using the configured PostScript distiller engine.

The *Convert to PDF using Outside In* option is selected on the Primary Web-Viewable Rendition page. When using this option, PDF conversion requires only a PostScript distiller engine.

26.1.2.1 PDF Export

PDF Export uses Outside In to export files directly to PDF without needing to first print to PostScript. By exporting to PDF directly, the use of a third-party distiller engine is not necessary.

26.1.3 XML Converter

Inbound Refinery includes Outside In XML Export and Search Export, which can be used to convert files to XML. This includes support for the following versions of the FlexionDoc and SearchML schemas:

- FlexionDoc

- SearchML

26.1.4 Outside In Technology

Oracle WebCenter Content uses Outside In Technology for many conversions, supporting many different format types. For detailed information about Outside In and supported formats, see the Outside In documentation:

http://www.oracle.com/technetwork/middleware/webcenter/content/ds-oitfiles-133032.pdf

For additional information on Outside In, see the Oracle Outside In Technology website at:

http://www.oracle.com/technetwork/middleware/webcenter/content/oit-all-085236.html.

26.2 File Formats Converted to PDF Using Third-Party Applications

When running on Windows, Inbound Refinery can use several third-party applications to create PDF files of content items. In most cases, a third-party application that can open and print the file is used to print the file to PostScript, and then the PostScript file is converted to PDF using the configured PostScript distiller engine. In some cases, Inbound Refinery can use a third-party application to convert a file directly to PDF.

The *Convert to PDF using third-party applications* option is selected on the Primary Web-Viewable Rendition page. When using this option, Inbound Refinery requires the following:

- A PostScript distiller engine.
- A PostScript printer.
- The third-party applications used during the conversion.
- WinNativeConverter component installed and enabled on the refinery server.

The following table lists the common file formats that can be converted to PDF using third-party applications on Windows. Please note the following important considerations:

- Third-party applications used in conversions, a PostScript distiller engine, and a PostScript printer are not provided with Inbound Refinery. You must obtain all third-party applications required for the conversions you want to perform, as well as a PostScript distiller engine and a PostScript printer of your choice.
- All third-party applications necessary to convert a file must be installed on the Inbound Refinery computer.
- Only the listed common file formats are supported for conversion. Conversion of additional file formats might be possible, however, the results cannot be guaranteed.
- Only the listed versions of each third-party application are supported for use with Inbound Refinery. Conversion using other versions of the third-party applications might be possible, however, the results cannot be guaranteed.

- Only conversion of listed file formats using the listed third-party applications is supported. Conversion of some file formats using an alternate third-party application might be possible (for example, conversion of Corel WordPerfect files using Microsoft Word), however, the results cannot be guaranteed.
- All listed file formats are supported for conversion to PDF, however, Outside In Image Export cannot create thumbnails from all of these native file formats. To ensure that thumbnails are created for all file formats, clear the *Create Thumbnail Image from the Native Vault File* check box on the Inbound Refinery Thumbnail Options page. When files are converted by Inbound Refinery and this check box is cleared, Outside In Image Export will create thumbnails from the generated web-viewable PDF files (instead of the native files), and therefore should be able to produce thumbnails for all files.

Common file formats that can be converted to PDF on a Windows Platform	**Supported 3rd-party applications for conversion**
Adobe FrameMaker *(see *below)* .fm .mif	Adobe FrameMaker 7.0
Adobe InDesign .indd .indt	Adobe InDesign CS2
Adobe PageMaker .pm# .pt# .p65	Adobe InDesign CS2
Adobe Photoshop .psd .eps	Adobe Photoshop CS2 *(see **below)*
Corel WordPerfect .wp .wp# .wpd	Corel WordPerfect 11
Microsoft Excel .xls .xlt .xlw .xlsx	Microsoft Excel (Office) 2003, 2007, 2010
Microsoft PowerPoint .ppt .pot .pps .ppa .pptx	Microsoft PowerPoint (Office) 2003, 2007, 2010
Microsoft Project .mpp	Microsoft Project (Office) 2003, 2007, 2010
Microsoft Publisher .pub	Microsoft Publisher (Office) 2003, 2007, 2010

Common file formats that can be converted to PDF on a Windows Platform	Supported 3rd-party applications for conversion
Microsoft Snapshot .snp	Microsoft Snapshot (Office) 2003, 2007, 2010
Microsoft Visio .vsd .vst .vdx .vtx	Microsoft Visio (Office) 2003, 2007, 2010
Microsoft Word .doc .dot .docx .dotx	Microsoft Word (Office) 2003, 2007, 2010
Microsoft Write .wri	Microsoft Word (Office) 2003, 2007, 2010
QuarkXPress .qxd .qxt	Adobe InDesign CS2
Rich Text Format .rtf	Microsoft Word (Office) 2003, 2007, 2010
Text .txt	Microsoft Word (Office) 2003, 2007, 2010

* Adobe FrameMaker+SGML is not supported. Adobe FrameMaker .book files are not supported.

** Adobe Photoshop CS2 requires manual configuration.

> **Note:**
>
> For important installation tips and recommended settings related to these third-party applications.

Part VI
Managing Dynamic Conversion

This part of the documentation discusses dynamic conversion of content.

Managing Dynamic Conversion contains the following chapters:

27

Introduction to Dynamic Converter

This chapter introduces Dynamic Converter, which is an Oracle WebCenter Content Server component that performs on-demand document conversion using templates which can be customized.
This chapter covers the following topics:

27.1 About Dynamic Converter

Dynamic Converter provides an industry-proven transformation technology and on-demand publishing solution for critical business documents. With Dynamic Converter, you can easily convert any business document into a web page for everyone to see without use of the application used to create that document. The benefits are immediate; information can be exchanged freely without the bottleneck of proprietary applications.

When a web browser first requests a document, a set of rules are applied to determine how that document should appear as a web page. These rules are defined in a template, a core component of Dynamic Converter.

Dynamic Converter offers a number of important benefits to users:

- Business documents can be easily viewed in a web browser.
- Native applications (such as Adobe Acrobat, Microsoft Word, etc.) are not required.
- Multiple renditions of a document are available for different web browsers.
- Numerous business document types, including legacy formats, are supported.

The HTML renditions of source documents in the Content Server are made available to users via an HTML link on the search results page and the content information page in the Content Server.

27.2 Basic Dynamic Converter Concepts

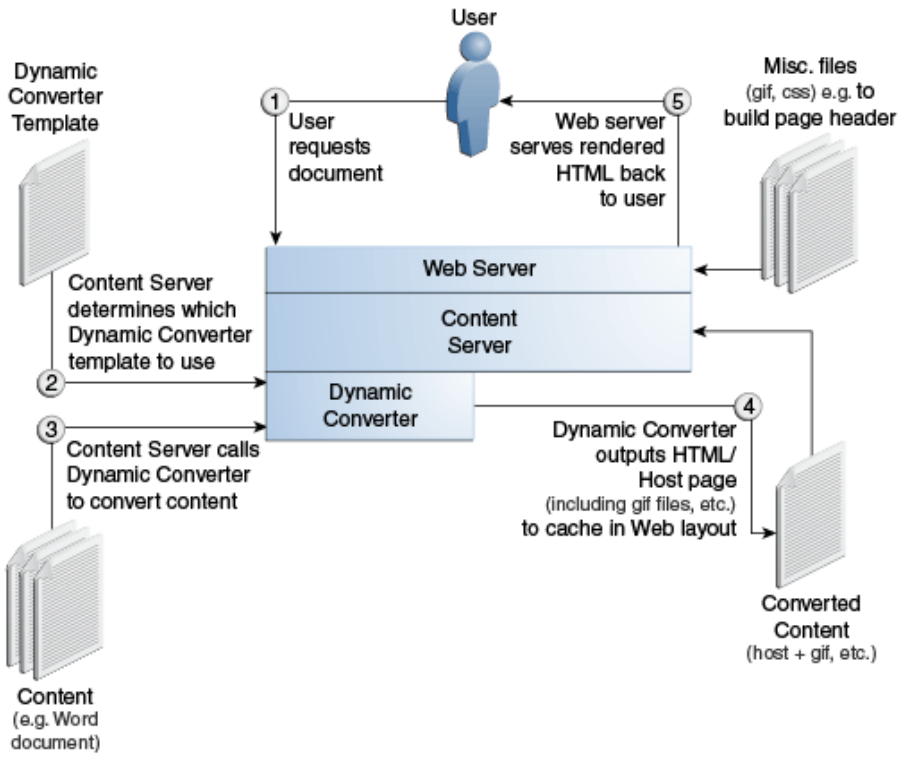
The following concepts are important in the context of Dynamic Converter:

- **Developer:** The individual who integrates Dynamic Converter into another technology or application.
- **Source file:** The document, spreadsheet, presentation or other information that the developer wishes to convert to a web page (also referred to as source document and content item).
- **Output file:** The file being created from the source file (also referred to as the web-viewable format).
- **Output files:** The complete set of files that together make up the rendered output (web page) from a source file.
- **Template:** A template tells the conversion engine how to convert the source document into the output document.
- **Template rules:** Documents matching certain criteria are converted using the specified template, layout, and options.

27.3 Dynamic Converter Process

Figure 27-1 shows the basic Dynamic Converter process.

Figure 27-1 Basic Dynamic Converter Process



The process consists of five steps:

1. A user requests a content item through a web browser.

2. The web server passes this request to Dynamic Converter, which determines the template to be used for the HTML conversion (based on metadata matching criteria).
3. Dynamic Converter converts the native file (for example, a Word document or Excel spreadsheet).
4. The conversion produces one or more HTML pages with supporting files (GIF, JPEG, and so on), which Dynamic Converter outputs to a special caching area in Content Server's web-viewable file repository ("Web Layout").
5. The web server retrieves any additional files (for example, CSS files or images used for the page header and footer), and serves these, together with all files produced by Dynamic Converter, to the user.

> **Note:**
>
> Dynamic Converter uses caching to reduce the load on the server and ensure that documents are not unnecessarily re-translated.

27.4 Upfront Conversions

In earlier versions of Dynamic Converter, a content item was converted to a web-viewable format (HTML, XML, etc.) when the content item was first requested by the user; more specifically, when the user clicked the (HTML) link beside the content item on the search results or content information page. Once the content item was converted, it was cached in the Content Server so that each subsequent request for the converted file would be immediate.

Since version 6.0 (circa 2004), Dynamic Converter can convert content items that match a conversion rule when the content item is checked in, rather than when the user requests it. As a result, users will be able to immediately view the dynamically converted rendition of the content item.

This upfront conversion applies only to content items that match a conversion rule in Dynamic Converter. Rules are specified on the Template Selection Rules page.

If no rule exists for the content item, then an upfront conversion will not take place, even if a default template and layout file are available for the content item. The default templates and layout files are specified on the Dynamic Converter Configuration page.

Please note that upfront conversions must be enabled in the Conversion and Caching Optimizations section of the Dynamic Converter Configuration page.

27.5 Forced Conversions

You can designate multiple conversions of the same content item so that it can be used for different purposes on your website. You might, for example, include it as a snippet of HTML code in one location and as a complete article in another location. This is done using a forced conversion in Dynamic Converter.

Forced conversions allow you to specify a list of rules where every rule is evaluated. If the first rule matches, it will be applied. If the next rule matches, it will also be applied, and so on. In this way, Dynamic Converter may create multiple renditions of the same content, if

necessary. As a result, content can be converted multiple times using different templates and layout files.

You can enable forced conversion for a template rule on the Template Selection Rules page.

A forced conversion takes place at the same time as an upfront conversion; that is, when the content item is checked into the Content Server. The end users will not be able to tell the difference between an upfront conversion and a forced conversion. Regardless of the method, the goal is the same: to have a content item converted and stored in cache by the time the user clicks the **HTML** link.

Please note that forced conversions must be enabled in the Conversion and Caching Optimizations section of the Dynamic Converter Configuration page, along with upfront conversions.

27.6 Fragment-Only Conversions

One type of forced conversion (see Forced Conversions) is the fragment-only conversion. A fragment is a piece of content that will be included in another content item. Individual fragments can then be combined to form a content-rich web page. A fragment generally contains no `<html>` or `<body>` tags, so that it can be easily included in another web page. The fragment is not intended to be viewed by itself and as such should not be displayed to users who click the **HTML** dynamic conversion link. Rules designed for fragments should be excluded from Dynamic Converter's rule evaluation during a user request.

When forced conversions are selected, you can enable fragment-only conversion for a template rule on the Template Selection Rules page.

Like other forced conversions, fragment-only conversions take place upfront, when the content item is checked into the Content Server.

27.7 Caching and Querying

Dynamic Converter includes a conversion and caching strategy that significantly improves the overall performance of your intranet or external website. This Element allows Content Server to serve up dynamically created web pages much more quickly than was possible in earlier versions.

While the conversion and caching enhancements are built into the application, there are several configuration options that you can set in order to fine-tune Dynamic Converter:

- Caching of Timestamps
- Metadata Changes
- Timestamp Checking Frequency
- Cache Interval
- Cache Size
- Cache Expiration Period

All these configuration options can be set in the Conversion and Caching Optimizations section of the Dynamic Converter Configuration page.

27.7.1 Caching of Timestamps

Every time a user clicks the **HTML** dynamic conversion link on the search results page or content information page, three files are queried in the Content Server database: the source document, the conversion template, and the layout file (if applicable). The database queries confirm that the dynamically converted file is the most recent, but these queries are done even when an up-to-date conversion is available.

Dynamic Converter version 6.2 and higher use a new method of verifying the revision of content items and conversion templates without querying the database each time. Instead, the time stamps of the converted content items are stored in the server's memory-based cache. Future conversion requests can then compare these cached time stamps with the time stamps of the content item to be converted without querying the database. When combined with the upfront conversion Element (see Upfront Conversions), Dynamic Converter becomes much more efficient in its revision and conversion queries. Using time stamps, the caching and querying mechanism detects the new revisions of content items in the Content Server, because with each new revision a new file is created with a new time stamp.

27.7.2 Metadata Changes

If you or your users make metadata-only changes to a content item, neither a new file nor a new time stamp is created, and the changes will go undetected. To address this problem, you must make sure that all metadata changes are identified by Dynamic Converter. You can do this by enabling the "Reconvert when metadata is updated" option on the Dynamic Converter Configuration page. This option forces the Content Server to update the time stamp of the source content items after a metadata update. With this option enabled, the time stamps of all web-viewable formats are updated to reflect the metadata change that occurred for the corresponding source content item. The updated time stamp, as a result, will be recognized by Dynamic Converter, and the content item, with metadata updates, will be reconverted.

Database Method of Checking

You can choose to use the database method of checking whether the content item's metadata has been updated. You set this option on the Dynamic Converter Configuration page. With this configuration option enabled, content item updates continue to signal timestamp changes in the converted files, but the new caching and querying method is not used to determine if the content items are up to date. Instead, the Content Server database is queried for this information. You might use this method, for example, if you are experiencing problems with the optimized query Element or you are troubleshooting a related issue.

27.7.3 Timestamp Checking Frequency

By default, Dynamic Converter checks the time stamp of the converted content items every 1,500 milliseconds, or 1.5 seconds. You can increase or decrease this value if you would like to balance the number of queries performed with the number of visitors to your site. You can change the timestamp checking frequency on the Dynamic Converter Configuration page.

If you increase this setting to, say, one minute (60,000 milliseconds) and a new content item is checked into the Content Server, then the new version will not be available to users until one minute has passed.

27.7.4 Cache Interval

The cache interval is the frequency with which the conversion cache is evaluated and cached items may be considered for deletion, depending on how long they have been in the cache and their conversion status. You can set the cache interval (in days) on the Dynamic Converter Configuration page. The default is seven days (once every week).

27.7.5 Cache Size

Dynamically converted files are kept in a cache to avoid unnecessary re-conversion. You can set the maximum cache size on the Dynamic Converter Configuration page. The default is 10,000 MB (about 10 GB). If the cache exceeds this maximum size, then during the next clean-up cycle (which, by default, is seven days) the cached items that have not been accessed for the longest period of time are deleted first. (The list for deleting is sorted by the "last accessed" date in ascending order.) If the cache size limit is not exceeded, then the cached items are examined for potential deletion in the same order, but items that are forced conversions of existing documents are not deleted.

27.7.6 Cache Expiration Period

Dynamic Converter keeps converted content items in the Web Layout conversion cache to prevent items from being reconverted unnecessarily. You can control the number of days that must pass before converted items in the cache may be considered for deletion. By default, cache clean-up is evaluated every seven days. Date expiration only applies to cached items for documents that are no longer present and to cached items that were not generated by forced conversion (see Forced Conversions). The default cache expiration period is seven days.

The cache expiration setting works in conjunction with the cache interval (see Cache Interval), which controls the frequency with which the cache is evaluated. For example, if the cache interval is set to 14 days and the cache expiration period is set to 8 days, then the cache will be evaluated every 14 days and all cached items older than 8 days will be deleted (unless they were the result of forced conversion).

27.8 Special Conversions

Dynamic Converter supports the following special conversions:

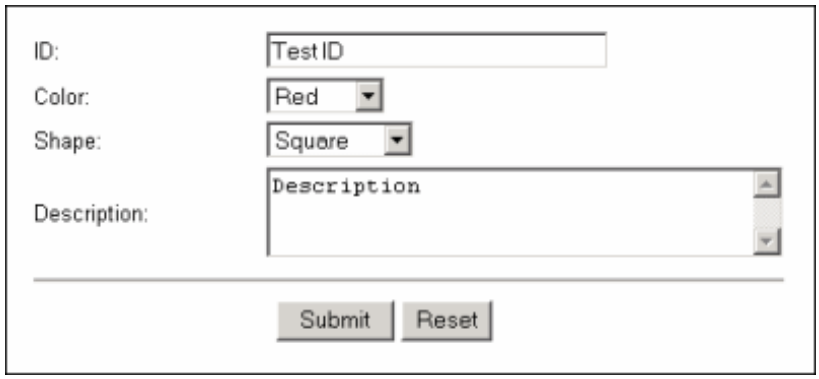
- Conversion of HTML Forms to HTML
- Conversion of XML to HTML

27.8.1 Conversion of HTML Forms to HTML

Dynamic Converter supports the conversion of HTML forms into HTML. This allows information supplied through HTML forms to be presented in flexible ways.

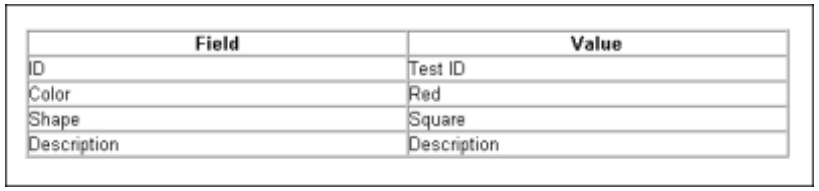
For example, the HTML form used to enter data might look something like this:

Figure 27-2 Data Entry Form



This HTML form, together with the values entered, is automatically checked into the Content Server as an HCSF file when it is submitted by clicking the Submit button. If a user then wants to view the form data, a template could be used to present the data from the HTML form.

Figure 27-3 Form Data in Table



Field	Value
ID	Test ID
Color	Red
Shape	Square
Description	Description

27.8.2 Conversion of XML to HTML

Dynamic Converter supports the conversion of XML to HTML by means of an XSL file. The XSL file (with the extension `.xsl`) is a template that defines how XML files are presented as HTML in a web browser.

In order for Dynamic Converter to properly identify and convert XML files, you must:

- Check the XSL file into the Content Server.
- Configure Dynamic Converter to recognize XML files. See Adding File Formats For Dynamic Conversion an explanation of how to add a file format for dynamic conversion. (In this case, you would add "application/xml" in the Formats text box.)
- Create a Dynamic Converter rule that matches the XML files you want to convert and specify the XSL file as the conversion template for that rule. For more information, see Managing Template Rules .

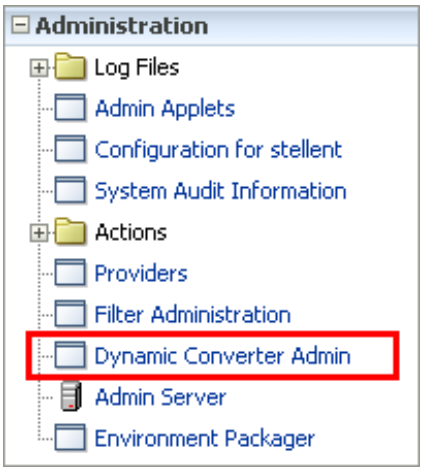
> **Note:**
>
> A sample XML file and XSL file are available for download from Oracle Technology Network at `http://www.oracle.com/technetwork/indexes/samplecode/`

27.9 Dynamic Converter Interface in Content Server

This section covers the changes to the Content Server interface after the Dynamic Converter software is installed.

If the Dynamic Converter Admin link is missing, the Dynamic Converter component was not correctly installed or enabled. For details on how to install the Dynamic Converter component, see Introduction in *Template Editor Guide for Dynamic Converter*.

Figure 27-4 Dynamic Converter Admin Link in Administration Tray



If Dynamic Converter was added to Content Server successfully, the Administration page and menu includes a link called **Dynamic Converter Admin**.

28
Configuring Dynamic Converter

This chapter describes how to set the Dynamic Converter default template, conversion formats, slideshow template files, and how to remove wireless templates.
This chapter covers the following topics:

28.1 Before Using Dynamic Converter

Before you begin using Dynamic Converter to design templates for your content items, the following must be in place:

- Content items checked into Oracle WebCenter Content Server. For information on how to check in content, see *Using Oracle WebCenter Content*.
- Dynamic Converter templates checked into Content Server with the correct template type. For more information, see Managing Conversion Templates .
- Template selection rules added, with associated metadata and templates. For more information, see Managing Template Rules .
- Conversion formats and other pertinent information specified on the Dynamic Converter Configuration page.

28.2 Setting the Default Template

A default template is applied to content items that do not match your defined template criteria. To change the default template associated with your content items:

1. Open the Dynamic Converter Admin page.
2. Click **Configuration Settings**.
3. On the Dynamic Converter Configuration page, in the **Template** text box under the Default Template heading, enter the content ID for a template. You can select the type of template from the **Template Types** menu and then choose your template from the **Available Templates** menu.
4. In the **Layout** text box, under the Default Layout heading, enter the content ID for a layout template. You can also choose your layout template from the **Available Layouts** menu. (Layouts only apply for the Classic HTML Conversion templates.)
5. Click **Update** at the bottom of the Dynamic Converter Configuration page to enable your default templates.

28.3 Setting Up Conversion Formats

The file format (MS Word, RTF, plain text, etc.) of your content items must be included in the conversion formats list in order for Dynamic Converter to recognize and convert the content item. Only file formats included in this list will have an **(HTML)** link beside them on the search results page, content information page, and so on.

This section covers the following topics:

- Adding File Formats For Dynamic Conversion
- Removing File Formats From Dynamic Conversion

28.3.1 Adding File Formats For Dynamic Conversion

You can add one or more file formats on the Dynamic Converter Configuration page at any time. To add a new file format:

1. Open the Dynamic Converter Admin page.
2. Click **Configuration Settings**.
3. On the Dynamic Converter Configuration page, under the Conversion Formats heading, in the formats text box, type the file format that you would like converted into a web page (or select it from the menu to the right). Formats in the text box must be separated by a comma and a space, for example:

   ```
   application/msword, application/vnd.ms-excel
   ```

   File formats must follow the naming convention in Content Server's Configuration Manager. For example, Microsoft Word documents are entered as *application/doc* or *application/msword*.

   Note that with Office 2007 files (for example, `docx`, `xlsx`, and `pptx`), you must enable the following formats on the DC Configuration page to see the **(HTML)** link:

   ```
   application/vnd.openxmlformats-officedocument.presentationml.presentation
   application/vnd.openxmlformats-officedocument.presentationml.slide
   application/vnd.openxmlformats-officedocument.presentationml.slideshow
   application/vnd.openxmlformats-officedocument.presentationml.template
   application/vnd.openxmlformats-officedocument.spreadsheetml.sheet
   application/vnd.openxmlformats-officedocument.spreadsheetml.template
   application/vnd.openxmlformats-officedocument.wordprocessingml.document
   application/vnd.openxmlformats-officedocument.wordprocessingml.template
   ```

   For more information on file format naming conventions, see the Content Server administration documentation.
4. Click **Update** to add your file formats to Dynamic Converter.

28.3.2 Removing File Formats From Dynamic Conversion

You can remove file formats on the Dynamic Converter Configuration page at any time. To remove a file format (you cannot undo this operation):

1. Open the Dynamic Converter Admin page.
2. Click **Configuration Settings**.

3. On the Dynamic Converter Configuration page, under the Conversion Formats heading, in the formats text box, select the file format that you would like to remove.
4. Press the **Delete** key on your keyboard to remove the file format from the text box. Be sure that you only remove the format that you wish to eliminate, and not all the formats listed in the box.
5. Click **Update** to remove the file format from Dynamic Converter.

> **Note:**
>
> If you accidentally delete the wrong file format, add it again, and then click **Update**.

28.4 Configuring Slideshow Template Files for PowerPoint Presentations

If you intend to use Dynamic Converter templates to convert PowerPoint presentations, it is recommended that you use an HTML Conversion template. You will be able to customize your template by navigating to **Document Formatting** then the **Presentations** tab in the template editor.

If you use a Classic HTML Conversion template, you should use the "slideshow" `hcst` files available for download from Oracle Technology Network at `http://www.oracle.com/technetwork/indexes/samplecode/`. After downloading, check the samples into Content Server. You need to check in all three of the slideshow files (`slideshow.hcst`, `slideshowb.hcst`, and `slideshowc.hcst`). A sample PowerPoint file (`dc_powerpoint.ppt`) is also available for download.

If you have Dynamic Converter configured in such a way that it automatically assigns content IDs upon file check-in, you need to edit each slideshow template file to reflect this. Each file must then be checked in again before you can begin using the templates.

To configure the slideshow template files for conversion of PowerPoint presentations:

1. Check all three slideshow files (`slideshow.hcst`, `slideshowb.hcst`, and `slideshowc.hcst`) into the Content Server. Make sure that you check them in as script templates. For more information, see Checking In a Template.

   To ensure the files are checked into the correct Web Layout directory, make sure that you use the same content type, security group, and account (if applicable) for all three files.

   If the content IDs are generated automatically, locate and note the automatically generated content ID of each slideshow file.

   If the content IDs are not generated automatically, it is recommended that you use something like "DC-Slideshow," "DC-SlideshowB," and "DC-SlideshowC."
2. Access the downloaded slideshow sample files.
3. Open each of the slideshow hcst files in a text editor, such as WordPad or vi, and then search for and replace the following slideshow references with the appropriate content IDs:

> **Note:**
>
> Be sure to save your changes before closing each file.

- **slideshow.hcst:**

  Search for: `slideshowbtemplate`

  Replace with: the content ID of the checked-in *slideshowb.hcst* template. For example, *1002* or *DC-SlideshowB*.

- **slideshowb.hcst:**

  Search for: `slideshowctemplate`

  Replace with: the content ID of the checked-in *slideshowc.hcst* template. For example, *1003* or *DC-SlideshowC*.

- **slideshowc.hcst:**

  Search for: `slideshowbtemplate`

  Replace with: the content ID of the checked-in *slideshowb.hcst* template. For example, *1002* or *DC-SlideshowB*.

  Make absolutely sure that you retain the file extension, so something like:

  ```
  {## link element=sections.current.bodyorimage
  template=slideshowbtemplate.hcst}.
  ```

  If you do not, the application may throw an exception during the HTML conversion.

  On UNIX systems, the content ID is case-sensitive, so `dc-slideshow` is not the same as `DC-Slideshow` or `DC-SLIDESHOW`.

4. Search for the slideshow files in the Content Server and click the **Info** link on the search results page.

   The content information page is displayed.

5. Click **Check out**.

6. Click **Check In** on the check-out confirmation page.

7. Browse to the modified slideshow files and click **Check In** on the content check-in form.

8. Repeat steps 4 to 7 for the each of the slideshow files.

You can now set up the conversion format for PowerPoint presentations (see Setting Up Conversion Formats) and assign the checked-in templates to a template rule (see Managing Template Rules).

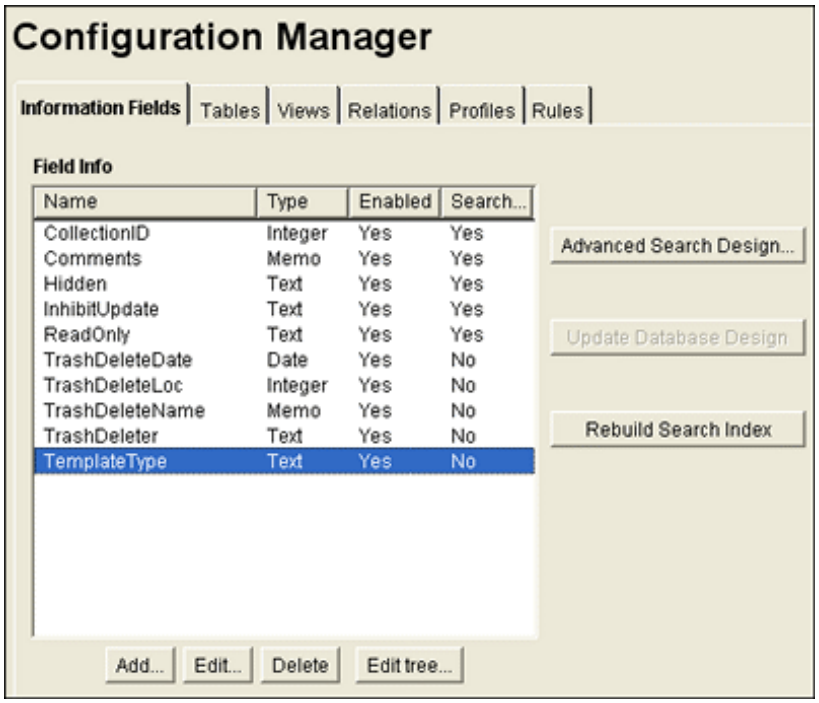
28.5 Removing Wireless Templates

Dynamic Converter 12.2.1 does not support the wireless template type, but still provides wireless support based on the Classic HTML Conversion templates. An existing Content Server with an earlier version of Dynamic Converter may still have the wireless template type, but attempting to use it will cause failure.

To remove the wireless template from the list of available templates:

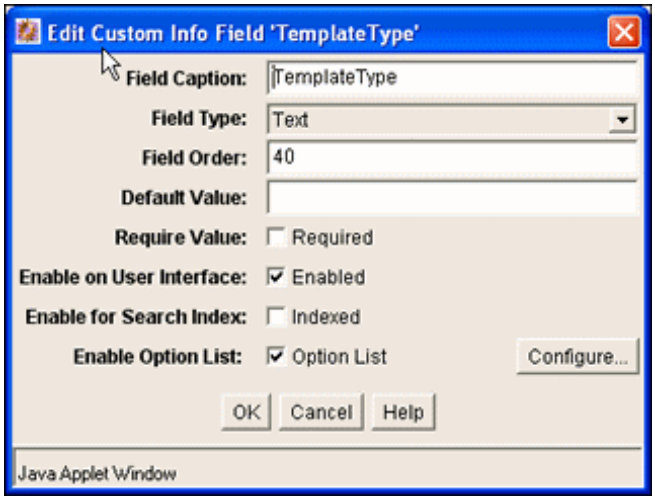
1. Open a new browser window and log into WebCenter Content as a system administrator.
2. Open the **Admin Applets** page.
3. Under the Administration Applets section, click **Configuration Manager**.

Figure 28-1 Configuration Manager Window



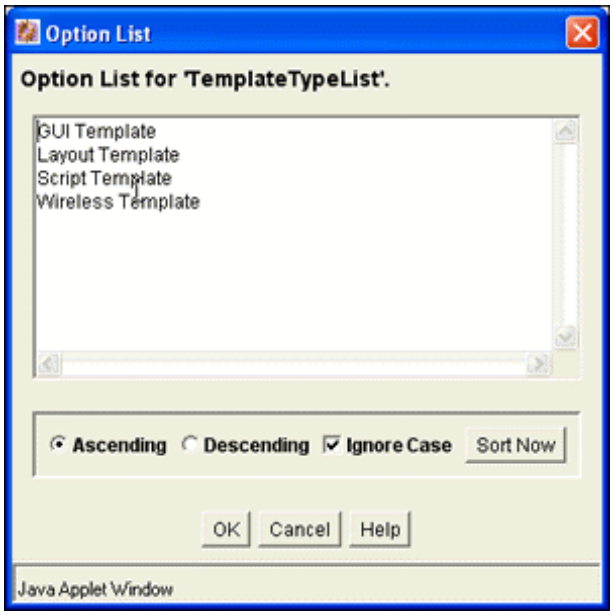
4. On the Configuration Manager window, on the **Information Fields** tab, choose the **TemplateType** row and click **Edit**.

Figure 28-2 Edit TemplateType Dialog



5. In the editing dialog for the TemplateType field, click **Configure**.
6. In the Configure Option List window, click **Edit**.

Figure 28-3 Option List for TemplateType



7. In the Option List window, highlight **Wireless Template** and press the **Delete** key to remove the Wireless Template as an option.
8. Click **OK** three times to return to the Configuration Manager window.
9. From the menu bar, choose **Options**.
10. Choose **Publish Schema**.

    Your changes are propagated to the Content Server.
11. Exit the Configuration Manager application and wait a few minutes. Then revisit the template check-in form.

29
Managing Template Rules

This chapter explains how to manage Dynamic Converter template rules, assign metadata criteria to a rule, and choose a temple for a rule.
This chapter covers the following topics.

- About Template Rules
- Managing Your Template Rules
- Assigning Metadata Criteria to a Rule
- Choosing a Template for a Rule

29.1 About Template Rules

A rule is a set of instructions that drive the conversion process in Dynamic Converter. These instructions identify source documents in the Content Server and then determine whether or not these documents should be converted based on their metadata (content ID, type, author, and so on) and file type. The rule then requests that the document be converted using the template associated with the rule (for more on templates, see Managing Conversion Templates). You can have more than one rule in Dynamic Converter. If this is the case, the first rule to match the source document's metadata is used for dynamic conversion. Depending on the system configuration, other matching rules may also be applied.

The Template Selection Rules page allows you to add, remove, and reorganize rules; specify the criteria (metadata) to base a rule on; and assign a template (or templates) to the rule.

A number of features have come together to form the Template Selection Rules page. You can add multiple rules and then change the order in which those rules will apply to source documents. You can select a number of metadata fields to base a rule on (and add even more fields using the configuration page). Lastly, you can assign a template (or templates) to the rule and then edit those templates using the Edit Template button.

29.2 Managing Your Template Rules

The top section of the Template Selection Rules page enables you to manage the template rules.

- Adding a Rule
- Deleting a Rule
- Reordering the Rules

29.2.1 Adding a Rule

To add a new template rule:

1. Open the Dynamic Converter Admin page.
2. Click **Template Selection Rules**.

3. On the Template Selection Rules page, type a name for your rule in the **New rule name** text box (under the Template Selection Rules heading).
4. Click **Add New Rule**.

   When your rule is highlighted, you will notice that the criteria and template fields for the rule are blank. You can start entering the metadata criteria and template for this rule right away.
5. Click **Update** at the bottom of the Template Selection Rules page.

29.2.2 Deleting a Rule

To delete a template rule from the Template Selection Rules list:

1. Open the Dynamic Converter Admin page.
2. Click **Template Selection Rules**.
3. On the Template Selection Rules page, highlight the rule to be deleted and click **Delete Rule**.
4. Click **Update** at the bottom of the Template Selection Rules page.

> **Note:**
>
> Deleting a rule will remove all of the settings (metadata criteria and template) for that rule. You cannot undo this operation.

29.2.3 Reordering the Rules

To change the order in which your template rules are processed:

1. Open the Dynamic Converter Admin page.
2. Click **Template Selection Rules**.
3. On the Template Selection Rules page, do either of the following:
   - To move a rule up the list, where it is prioritized over other rules, highlight the rule and click **Move Up**. Then click **Update**.
   - To move a rule down the list, where it will receive a lower priority, highlight the rule and click **Move Down**. Then click **Update**.

29.3 Assigning Metadata Criteria to a Rule

When assigning conversion templates to content items, you need to make sure that the metadata specified here matches the metadata assigned to your source documents. You can verify this by opening the content information page for your source documents in the Content Server.

To assign metadata to a template selection rule:

1. Open the Dynamic Converter Admin page.
2. Click **Template Selection Rules**.

3. On the Template Selection Rules page, choose a metadata field from the first **Field** list (under the "Criteria for selected rule" heading). You may choose Type, Author, Title, Content ID, Title, or a number of other fields.
4. In the **Value** text box, enter the metadata that you would like your rule to target.

   You can select the metadata value from the menu to the right of the Value text box. You can also use wildcards to specify a metadata value.
5. You have the option to choose a second and third metadata field for your rule.

   There will always be an "AND" relationship between the metadata fields, which means that only those content items that meet ***all*** criteria are converted by this rule.

   The maximum number of criteria that you can specify for each rule is controlled by a setting on the Dynamic Converter Configuration Page.
6. Click **Update** on the bottom of the Template Selection Rules page to update your rule.

29.4 Choosing a Template for a Rule

Your template selection rule is not complete until you choose a template for the rule. The template will ultimately drive the appearance of your converted documents.

To assign a template to a rule:

1. Open the Dynamic Converter Admin page.
2. Click **Template Selection Rules**.
3. On the Template Selection Rules page, enter the content ID for the template in the **Template** text box (under the "Template and layout for selected rule" heading).

   You can select a type of template (HTML Conversion, Classic HTML Conversion, or Script) from the **Template Types** menu, and then you can select your template from the **Available Templates** menu.
4. If you chose a Classic HTML Conversion template in the previous step, you may want to complement it with a layout template. If so, enter the content ID for the layout template in the **Layout** text box (again, you may select the layout template from the **Available Layouts** menu).
5. Click **Update** to add the template to your rule.

Once you have created a template selection rule, assigned the appropriate metadata criteria to it, and selected a template (or templates) for the rule, you should verify your configuration settings on the Dynamic Converter Configuration page. In particular, make sure that you have added the necessary file types to the Conversion Formats list.

For more information, see Managing Conversion Templates .

30
Managing Conversion Templates

This chapter provides information about Dynamic Converter templates, template types, and how to check in a template.
This chapter covers the following topics:

- About Templates
- Template Types
- Template Strategy
- Checking In a Template

Related Topics

- HTML Conversion Templates
- Classic HTML Conversion Layout Templates
- Managing Script Templates

30.1 About Templates

Much of the power, flexibility, and complexity of Dynamic Converter is bound up in its use of templates to drive the conversion process. Templates give you immense control over the visual and navigational properties of the converted web page.

A template is a plain-text HTML or XML file that may include special tags which allow template writers to insert, repeat through, condition on, and link to various elements in the source document. You can associate these sets of formatting instructions with one or multiple content items that are stored in the Content Server. When you assign a template to your content items (on the Template Selection Rules page), you are controlling the way your content items will appear as web pages.

When users click the **(HTML)** link (generated by Dynamic Converter) for a content item, a dynamic conversion takes place using the template associated with that content item (see Process).

30.2 Template Types

There are four types of templates available in Dynamic Converter:

- **Classic HTML Conversion templates**: Classic HTML Conversion templates (formerly known as GUI templates) are written in XML (Extensible Markup Language) and are designed for use with the Dynamic Converter Classic HTML Conversion Editor. The Classic HTML Conversion Editor is not available in 12*c*. Templates created in earlier versions can still be used, but cannot be created or edited in 12*c*. Classic HTML Conversion templates have the `.ttp` file extension. For more information, see HTML Conversion Templates .
- **HTML Conversion templates**: The HTML Conversion Editor's primary goal is producing faithful representations of source files using the HTML, GIF, JPEG, and PNG formats.

Using a C API and a powerful, customizable XML file, you can use the HTML Conversion Editor to set various options that affect the content and structure of the output. The HTML Conversion Editor is Java-based and can run in any browser instance where a JRE is present. For more information, see HTML Conversion Templates .

- **Classic HTML Conversion Layout templates**: Layout templates are designed to complement GUI templates in that they control the overall page layout for converted content items. A layout template can be used to create a common set of borders, site navigation, or a company logo on each converted web page. It can also be used to maintain the Content Server look and feel with links to Home, Search, etc. Layout templates typically contain HTML code (especially HTML tables), tokens (which represent GUI template settings), and Idoc Script or a different scripting language. For more information, see Classic HTML Conversion Layout Templates .
- **Script templates**: Script templates are text-based conversion templates that apply a set of scripted rules to your converted documents. They are plain-text files that must be hand-coded with elements, indexes, macros, pragmas, and Idoc Script. Changing script templates requires a knowledge of the language that they were written in. Script templates have the `.hcst` file extension. For more information, see Managing Script Templates .

30.3 Template Strategy

Through the use of templates, Dynamic Converter users have infinite flexibility in the way they can present converted documents. Users typically use one of the following three strategies to select a template:

1. A number of sample templates designed to meet different needs for Dynamic Converter users (polished navigation, simple HTML for document indexing engines, etc.) are available for download from Oracle Technology Network at `http://www.oracle.com/technetwork/indexes/samplecode/`. .
2. With a bit more effort, you can modify one of the sample templates available for download from Oracle Technology Network. Simple changes, such as adding graphics or static text, should be easily accomplished by someone with a willingness to experiment with these templates.
3. Advanced users may choose to write a template of their own design, customized specifically to their needs. Such templates can incorporate elements from a wide range of Web standards, such as Java. Needless to say, users who go this route should have strong technical skills at the outset.

30.4 Checking In a Template

You need to check a template into the Content Server before it can be assigned to a template selection rule (see Managing Template Rules) and used by Dynamic Converter in the conversion process.

To check in a template:

1. Open the Dynamic Converter Admin page.
2. Click **Check In Existing Template**.
3. On the Template Check-In Form, specify all required metadata for the template.

Make sure that you select the correct template type. If you do not, a template may not be included in the list of available templates of a particular type. If that is the case, you need to open the content information page of the checked-in template and update its template type.

4. When you are done, click **Check In** to check the template file into the Content Server.

For more information about checking content into the Content Server, see *Using Oracle WebCenter Content*.

31
HTML Conversion Templates

This chapter provides information about HTML (graphical user interface) templates and how to use the template editor for Dynamic Converter.
This chapter covers the following topics:

- About Templates
- Using the HTML Conversion Template Editor

31.1 About Templates

A template is a set of formatting instructions you can associate with a source document. When you check a document into Content Server, you either associate it with a default conversion template, or you can create a new customized template.

The following template options are available:

- **HTML Conversion templates**: These are the newest template types, which can be configured in a cross-platform editor.
- **Classic HTML Conversion templates**: These were previously known as GUI templates. There is no direct migration path from the GUI templates to the HTML Conversion templates. If you select a Classic HTML Conversion template, you may also select a Classic HTML Conversion layout.
- **Script templates**: These run with default settings, and can be edited with a text editor.

After you have chosen a template type to associate with your document, and named the template, you can edit the template. There is a template editing utility called the HTML Conversion Editor which can be used to edit the HTML Conversion Templates. This utility allows you to customize the appearance of native documents converted to an HTML format. This template editor is used to control the look and feel of the web pages you create. The Classic HTML Conversion Template Editor is not available in WebCenter Content 12*c*. Templates created in earlier versions can still be used, but cannot be created or edited in 12*c*.

To turn a source document into a web page, you can use the default settings to perform a conversion. Alternatively, you can create an HTML template, associate it with the document, and then edit the template using the HTML Conversion Editor.

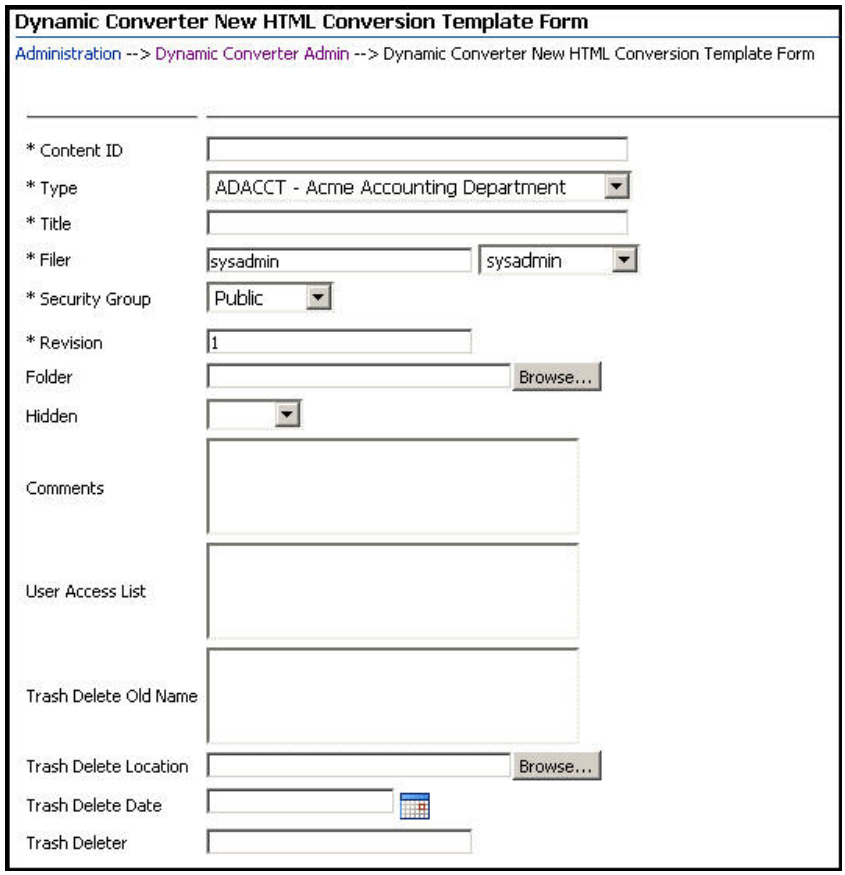
The following sections describe tasks for the HTML Conversion Editor:

- Creating a New HTML Conversion Template
- Editing an Existing HTML Conversion Template

31.1.1 Creating a New HTML Conversion Template

Use the Dynamic Converter New HTML Conversion Template Form to create a new HTML Conversion Template. To access this page, click **Create New Template** on the Dynamic Converter Admin page.

Figure 31-1 New HTML Conversion Template Form



> **Note:**
>
> For more information about checking content into the Content Server, see *Using Oracle WebCenter Content*.

To create a new HTML Conversion template:

1. Open the Dynamic Converter Admin page.
2. Click **Create New Template**.
3. Specify all other required metadata for the template.
4. When you have completed the form, click **Check In** to check the HTML Conversion template file into the Content Server.

After checking a new HTML Conversion template into the Content Server, you can edit it using the Template Editor (see Editing an Existing HTML Conversion Template).

31.1.2 Editing an Existing HTML Conversion Template

The HTML Conversion Template Editor requires Internet Explorer on a Windows XP or greater system. To edit an existing HTML Conversion Template (that is, one that is already checked into the Content Server):

1. Open the Dynamic Converter Admin page.
2. Click **Edit Existing Template**.
3. On the Edit Templates page, select a template from the list of HTML Conversion templates in the Content Server.

   If a known HTML Conversion template is not included in the list of available templates, then it was most likely not assigned the correct HTML Conversion Template type when it was checked into the Content Server (see Checking In a Template). You then need to open the content information page of the checked-in template and update its template type.

   The Edit Template button does not become available until you specify the name of an existing template.
4. Click the **Edit Template** button. The HTML Conversion Template Editor is downloaded to your machine. With some browsers, such as Firefox, you may be prompted for how to handle the file `dc_hcmapedit.jnlp`. The correct way to open this file is with Java (TM) Web Start Launcher (default).

   The Template Editor is started. If you have not run the editor before, it is installed first and you may need to confirm a few prompts.

You can now edit the HTML Conversion template in the Template Editor.

You can also edit an existing HTML Conversion template from the Template Selection Rules page.

> **Note:**
>
> The Template Editor comes with its own extensive help system, which can be called from the application's user interface.

31.2 Using the HTML Conversion Template Editor

This section provides a description of the HTML Conversion Template Editor. More detail can be found in *Template Editor Guide for Dynamic Converter*.

The HTML Conversion Editor allows you to set various options that affect the content and structure of the output. The HTML Conversion Editor is Java-based and can run in any browser instance where a JRE is present.

The following topics are covered in this section:

- Formatting Different File Types
- Adding Document Properties
- Adding Text Elements

- Adding Navigation Elements
- Configuring HTML Settings
- Adding Output Markup Items
- Adding Output Text Formats
- Adding Format Mapping Rules
- Adding Output Page Layouts
- Previewing Your Content
- Saving Your Template

31.2.1 Formatting Different File Types

The top item in the left-hand navigation pane of the HTML Conversion Editor allows you to set up custom formatting for different file types. Each file type uses a layout, either the default layout, or one created under Output Page Layouts. The exported files will use the same template as the root conversion.

These file types have slightly different options for formatting:

- **Text/Word Processing**: Allows you to set options for bullets, footnotes and endnotes, handling character styles and embedded graphics, and setting pagination.
- **Spreadsheets**: Allows you to set up section formatting and labeling, display grid lines, and size embedded graphics.
- **Presentations**: Allows you to set up section formatting and labeling, and size slides.
- **Images**: Allows you to set up section formatting and labeling, and size images.
- **Archives**: Allows you to display either Filenames (the names of files and folders in the archive will be output) or Decompressed files (the file names will be output as links to the exported files). The exported files use the same template as the root conversion.
- **Database**: Allows you to set up section formatting and labeling, and set the number of records per page.

31.2.2 Adding Document Properties

This item allows you to add predefined and custom properties. You can assign default values, metatag names, and output format to these properties

By default, no document properties are defined. In order to include them in the output from the conversion, each document property must first be defined here. They must then be added to the output from the conversion by inserting them into page layouts defined in the Output Page Layouts item.The most common predefined properties are as follows:

- Primary author
- Title
- Subject
- Keywords

- Content

Several more less common predefined properties are also available.

For a custom property, you can create a descriptive name, and then assign default values, metatag names, and output formats.

31.2.3 Adding Text Elements

Text elements allow the user to insert strings into the output. Each text element is defined as a name-value pair with an optional output format that will be used to format the text.

If an output format is not specified, the text will be inserted into the output as-is, with no additional markup.

31.2.4 Adding Navigation Elements

Navigation elements allow you to have navigation links generated in the output. There are three kinds of navigation elements:

- **Document Navigation**: This allows you to link to various items in the source document based on the document's structure. A common example of how one would use this type of navigation is to create links to all the paragraphs marked with outline level 1 (such as "Heading 1" paragraphs) in the document. Before using this form of navigation, link mapping rules must first be added. Link mapping rules establish which parts of the input document will be used to create links.
- **Page Navigation**: This provides a way to link to certain key pages in the output (first page, next page, and so forth). It also provides a way to link to external pages.
- **Section Navigation**: This provides navigation for multi-section documents, such as spreadsheets and presentations.

Once you have added one of these, the left hand side of the editor displays expanded levels. You can specify information about the link, link set markup and formatting, and create link mapping rules. Link mapping rules allow you to match on a paragraph outline level or paragraph style name in order to generate navigation based on these two aspects of the source document. Once you define rules, click back on the Link Mapping Rules page to determine the sequence of the rules. The mapping rules are ordered so that the first rule that matches is the one that is applied.

31.2.5 Configuring HTML Settings

There are six major categories that you can configure:

- **HTML Settings**: Allows you to set the HTML DOCTYPE and Language string.
- **CSS options**: Allows you to specify whether Cascading Style Sheet ("CSS") formatting will be used, and if so, the method of CSS presentation. By default, the CSS is embedded in the HTML of each output file. You may also choose to output CSS styles in a separate file. The external stylesheet option allows you to specify a stylesheet with user-generated styles that will be referenced by the conversion.
- **Character set**: Allows you to specify which character set should be used in the output file. Source documents that contain characters from many character sets will look best only when this option is set to Unicode or UTF-8. You may also select a character to be used when a character cannot be found in the output character set (unmappable).

- **Graphics output**: Allows you to specify the format of the graphics produced by the technology: GIF, JPG, PNG, or none. Other options in this section allow you to specify quality and sizing of the graphic output.
- **Link options**: This option allows you to specify how the browser should select which frame or window in which to open source document links. This value is used for the target attribute of the links the technology generates. This target value will be applied to all such links encountered in the source document.
- **Output formatting**: This option causes the technology to write new blank lines to the output strictly to make the generated HTML more readable and visually appealing. While setting this option will make it easier to read the generated markup in a text editor, it does not affect the browser's rendering of the document. You can also include information about source document style names and how they are mapped, and the user can see what format has been mapped to a particular paragraph or text sequence by mousing over it.

31.2.6 Adding Output Markup Items

Markup items are HTML fragments that may be inserted directly into the output HTML as part of a page layout (see Adding Output Page Layouts). Each markup item is a name/value pair. The name is what will appear in the screens for editing page layouts. The value is a block of HTML that will be inserted into the output HTML wherever the markup item appears in a page layout.

Click the **Add** button and specify a **Name** to use for referencing this piece of markup. Then enter the HTML into the **Markup** text box.

31.2.7 Adding Output Text Formats

Output text formats define text and formatting attributes of output document text. This allows you to standardize the look of the output despite differing formatting styles used by the various authors of the source documents. Text formats are only applied to text from word processing files. They cannot be used to change the formatting of text that is rendered as part of any graphics generated by the conversion. They are also not applied to text inside spreadsheets.

1. Click the **Add** button to display the Markup tab, then specify a **Name** to use for referencing this format.
2. Under **Tag name**, enter the HTML paragraph level tag to put around paragraphs using this format. Note that any tag name may be entered here, whether it is legal or not. Only the tag name should be entered, not the surrounding angle brackets ("<" and ">"). The paragraph tag ("p") is the default.
3. Under Custom Attributes, you can enter attributes that apply to the tag whose name was specified by the **Tag name** option above. To set the name and value of the new attribute, just click on them in the Custom Attributes table.
4. Custom Markup allows you to enter HTML and/or regular text that will be inserted before and/or after every paragraph using this format.
5. Other formatting options on the Markup tab include inserting new lines into the HTML before the paragraph to make it easier to view the HTML of the output of the conversion (only written if the **Format HTML source for readability** option is set on the Output Pages screen); specifying that a new output page is created every time this format is applied to a paragraph; and whether or not the first

instance of this format should start a new page (to help avoid empty or mostly empty pages at the beginning of the output).

6. On the Formatting tab, you can choose how to specify the formatting for paragraphs. If you click on the **Use external CSS class** option, a text field becomes available in which you must enter the name of a class from an external CSS file. The URL of the external CSS file is specified with the **External user stylesheet** option set on the Output Pages page.

   If you do not specify an external stylesheet, you can choose to format the document by observing the original source document formatting or forcing other formatting options. Character, Paragraph and Border formatting for an array of options can be set to one of four values:

   - **Always off**: Forces the attribute to always be off when formatting the text.
   - **Always on**: Forces the attribute to always be on when formatting the text.
   - **Inherit** (default): Takes the state of the attribute from the source document. In other words, if the source document had the text rendered with bold, then the technology will create bold text.
   - **Do not specify**: Leave the formatting unspecified.

31.2.8 Adding Format Mapping Rules

Once you have defined text formats, you must define rules to map output text formats to output text.

1. Select Format Mapping Rules and click **Add Format Mapping Rule**.
2. In the **Format** box, select one of your defined text formats.
3. In the **Match on** box, you may select one of the following paragraph formatting options for the rule to check:
   - **Outline level**: Match the outline level specified in the source document. Application-predefined "heading" styles typically have corresponding outline levels applied as part of the style definition.
   - **Style name**: Match the paragraph or character style name.
   - **Is footnote**: Match any footnote.
   - **Is endnote**: Match any endnote.
   - **Is header**: Match any document header text.
   - **Is footer**: Match any document footer text.
4. For the Paragraph outline level, if **Match on** above is set to **Outline level**, then this defines which outline level to match. This option cannot be set/is ignored for all other matching rules.
5. If **Match on** above is set to **Style name**, then this defines which source document paragraph or character style name to match. When matching on style names, you must supply a style name here, and no default value is provided. The name must exactly match the style name from the source document. Style name matching is done in a case-sensitive manner. This option cannot be set/is ignored for all other matching rules.
6. When you have finished defining rules, you can go back to the Format Mapping Rules page and click on **Move Up** or **Move Down** to arrange the sequence in which the rules

are checked. The mapping rules should be ordered so that the first rule that matches is the one, and only one, that is applied.

31.2.9 Adding Output Page Layouts

The Output Page Layouts section allows you to define the content of a set of output files. Page layouts are used to organize how the various pieces of the output are arranged.

1. Click **Add** to add a new output page layout. On the next page, enter a name to use to refer to this layout (required). Once this has been done, click on the left side of the editor. The name you have just entered is displayed in the tree view. Click on this to expand the levels underneath.
2. Click the box in front of **Include navigation layout** if you want to generate a single file containing markup and links to the document content specified in the page layout. This allows the user to create a "table of contents" page. You will need to define a navigation element under the Navigation Layout.
3. The first item under the name of your output page layout is <title> Source. This lets you select where to get the value to use for the HTML <title> tag. Select Section Name, Text Element, Property, or Output Text Format (the last three must be previously defined). Click back on the <title> Source page to order the sequence of these sources.
4. The Navigation Layout triggers the creation of a separate file with nothing but links to the actual document content. In order to generate this, you must have previously defined either a Document Navigation, Page Navigation, or Section Navigation element under Generated Content (see Adding Navigation Elements). In the expanded level under Navigation Layout, you can further select Markup Items to be placed in the Head and/or Body of the navigation page.
5. The top level of the Page Layout section lets you set pagination options. The six options under Page Layout let you define how output documents are arranged. These six options are as follows:
   - **Head**: Items placed in the HTML <head> of each output file.
   - **Page Top**: Items to be placed at the top of each output page. For example, links to the first page, previous page and next page in the output.
   - **Before Content**: Items to be output before the document content.
   - **Before Section**: Items inserted before each section of a multi-section document. Note that this is not applicable to word-processing documents.
   - **After Content**: Items to be output after the document content.
   - **Page Bottom**: Items placed at the top of each output page; for example, a copyright notice.

   After selecting items to display for these six options, click at the top level of each one to set the order in which they will appear.

31.2.10 Previewing Your Content

The HTML Conversion Editor provides two options for previewing your content. They are both located in the Tools menu at the top of the interface.

- **View XML Structure**: Click this option to display the XML structure viewer, which shows a text-based XML version of your chosen template options.
- **Set preview document**: Click this option to enter the Content ID of the source document, and then click **Preview Conversion**. Your browser will open and display how the current template settings would affect the converted output.

31.2.11 Saving Your Template

If you start to exit the template editor, you will be prompted to supply an XML filename and location to store your template.

32
Classic HTML Conversion Layout Templates

This chapter provides information about creating and using classic HTML conversion layout templates.
This chapter covers the following topics:

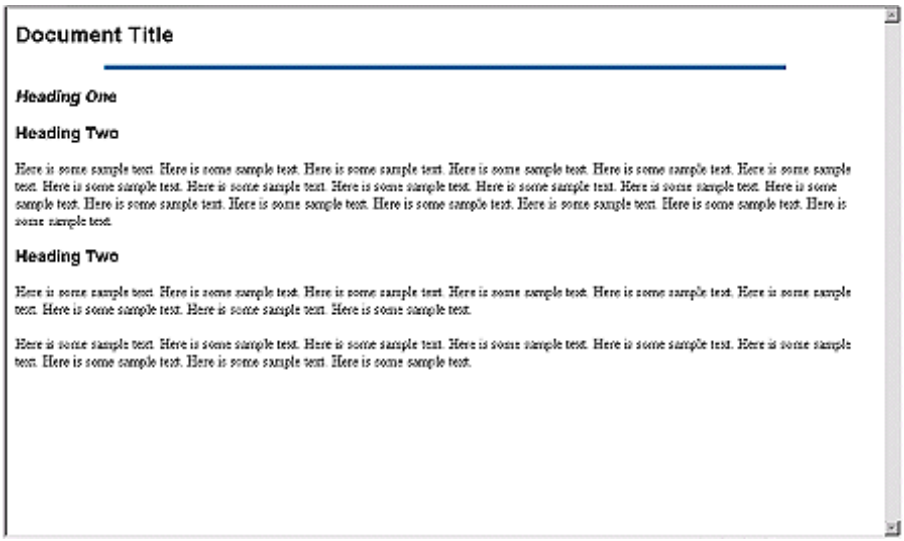
32.1 About Classic HTML Conversion Layout Templates

Layout templates can be used to complement Classic HTML Conversion templates (see HTML Conversion Templates). They can be used to control the placement of items on a web page, in particular, the areas outside of the converted document. You can add shared borders, navigation, custom scripting, and much more in your layout template. You might use the layout template to create a common set of links around your converted documents (such as "additional resources"), or you might prefer to maintain the Content Server look and feel around your documents using Idoc Script header and footer tags.

> **Note:**
>
> The Classic HTML Conversion Template Editor is not available in WebCenter Content 12*c*. Templates created in earlier versions can still be used, but cannot be created or edited in 12*c*.

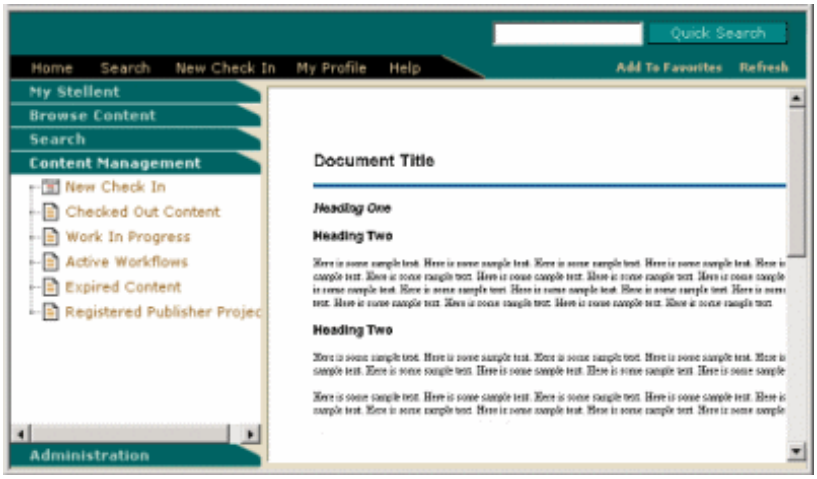
If you do not specify a layout template on the Template Selection Rules page, your converted document will take up the entire web browser screen area when a user clicks the **(HTML)** link in the Content Server interface (see Viewing a Converted File).

Figure 32-1 Converted Document without Layout Template



If you specify a layout template, such as the `default_layout.txt` sample, you can add a consistent look and feel around your content items.

Figure 32-2 Converted Document with Layout Template



32.2 Layout Template Contents

A typical layout template contains the following parts:

- HTML top and head information
- HTML tables (used to control page layout)
- Tokens for your template settings (see Tokens in Layout Templates)
- Idoc Script code (for various purposes)

When used together, you will find that you can fine tune the appearance of your converted documents on a global level, giving your online information a professional and consistent look and feel.

32.3 Tokens in Layout Templates

Tokens are placeholders or variables for the Classic HTML Conversion template settings that you create in the Template Editor. A layout template is used to control the placement of items around your converted content. If you wanted to include a particular TOP or HEAD setting from your Classic HTML Conversion template (keep in mind that layout templates are frequently used with Classic HTML Conversion templates), this would normally require you to copy and paste the information into your layout template (in the TOP or HEAD HTML tag). With a token, you can reserve that space for a Classic HTML Conversion template setting.

There are four tokens available:

- **<!--TRANSIT - CUSTOMLAYOUT(TOP)-->**

  Place this token at the top of the layout template before the <HTML> tag. Your template could replace this value with an HTML declaration, such as the W3C document type identifier.

- **<!--TRANSIT - CUSTOMLAYOUT(HEAD)-->**

  Place this token between the <HEAD> tags. Your template could replace this value with a web page title, meta tag keyword, and much more.

- **%%TRANSIT-BODYATTRIBUTES%%**

  Place this token in the <BODY> tag. Your template could replace this value with a background color, text color, link behavior, and much more.

- **<!-- TRANSIT - CUSTOMLAYOUT(BODY) -->**

  Place this token at the location where you would like your actual content items to appear on the web page. You will likely place this somewhere in the middle of your layout template. Your template will replace this value with each content item. This token can be used by itself to generate minimum HTML output so that the content item can be included in another web page.

32.4 Sample Layout Templates

A number of sample layout templates are available for download from Oracle Technology Network at `http://www.oracle.com/technetwork/indexes/samplecode/`. After downloading, check the sample into Content Server to begin using.

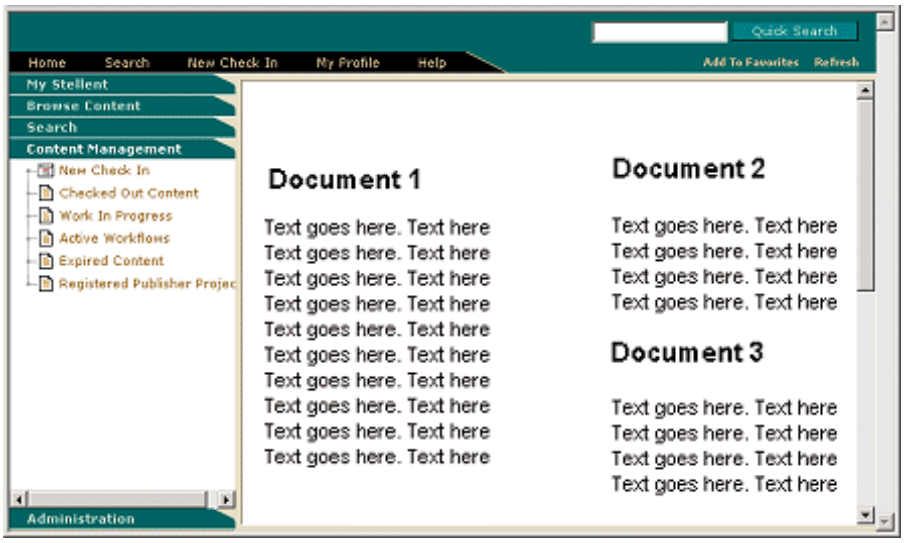
The following sample layout templates are available:

- default_layout.txt
- snippet_layout.txt

32.4.1 default_layout.txt

The `default_layout.txt` template wraps Content Server borders and navigation around your converted documents using Idoc Script and HTML tables.

Figure 32-3 Default Layout



The `default_layout.txt` layout template contains the following code:

```
<html>
<head>
<!-- TRANSIT - CUSTOMLAYOUT(HEAD) -->
<$defaultPageTitle="Converted Content"$>
<$include std_html_head_declarations$>
</head>

<$include body_def$>
<$include std_page_begin$>
<$include std_header$>

<table border="0" cellpadding="0" cellspacing="0" width="550">
<tr><td>

<!-- TRANSIT - CUSTOMLAYOUT(BODY) -->

</td></tr>
</table>

<$include std_page_end$>

</body>
</html>
```

32.4.2 snippet_layout.txt

The `snippet_layout.txt` template places the converted document on a web page, by itself, without the top, head, or body HTML markup. The result is very similar to what happens when there is no layout template associated, but the advantage here is that you can easily pull this content into another web page, possibly a portal site, as an HTML snippet.

The `snippet_layout.txt` layout template consists of a single line of code:

```
<!-- TRANSIT - CUSTOMLAYOUT(BODY) -->
```

This is a token that displays the actual content item on the web page. Because it used by itself here, minimum HTML output is generated which can be included in another web page or HTML snippets.

Snippet Demo

The `snippet_demo.hcst` sample includes the basic ingredients for a portal-style web page that draws information (HTML snippets) from other content items stored in the Content Server, while preserving the borders and navigation.

The `snippet_demo.hcst` sample contains the following code:

```
<html>
<head>
<meta http-equiv="Content-Type" content="text/html; charset=iso-8859-1">
<title>This is my incDynConv script test page</title>
<meta name="GENERATOR" content="Dynamic Converter">
<$defaultPageTitle="Converted Content"$>
<$include std_html_head_declarations$>
</head>

<$include body_def$>
<$include std_page_begin$>
<$include std_header$>

This is a sample page that shows how to include multiple snippets of dynamically<br>
converted content on a single page using the new Idoc function incDynamicConversion.

<table border="1" cellpadding="0" cellspacing="0" width="550">
 <tr>
 <td>

<$incDynamicConversion("<source_contentID_1>","latest","<template_contentID_1>","snippe
t_layout")$>
 </td>
 <td>

<$incDynamicConversion("<source_contentID_2>","latest","<template_contentID_2>","snippe
t_layout")$>
 </td>
 </tr>
 <tr>
 <td colspan=2>

<$incDynamicConversion("<source_contentID_3>","latest","<template_contentID_3>","snippe
t_layout")$>
 </td>
 </tr>
</table>

<$include std_page_end$>

</body>
</html>
```

32.5 Creating a Layout Template for Your Content Items

To create and edit a layout template:

1. Create a new layout template in a text editor or WYSIWYG tool. For information on the contents of a layout template, see Layout Template Contents.

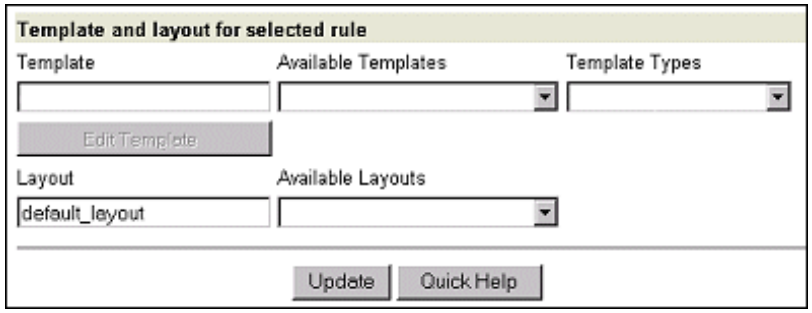
> **Note:**
>
> A number of sample layout templates are available for download from Oracle Technology Network at `http://www.oracle.com/technetwork/indexes/samplecode/` that you can use as a starting point (see Sample Layout Templates).

2. Open the Dynamic Converter Admin page.
3. Click **Check In Existing Template** and follow the steps to check in an existing template (see Checking In a Template). Make sure that you choose **Layout Template** as the template type.
4. Return to the Dynamic Converter Admin page.
5. Associate your layout template with a template rule (see Associating a Layout Template With a Template Rule).

32.6 Associating a Layout Template With a Template Rule

You can associate a particular layout template with a template rule on the Template Selection Rules page. In the example below, the template sample titled "default_layout" has been selected.

Figure 32-4 Selection of Layout Template on Template Selection Rules Page



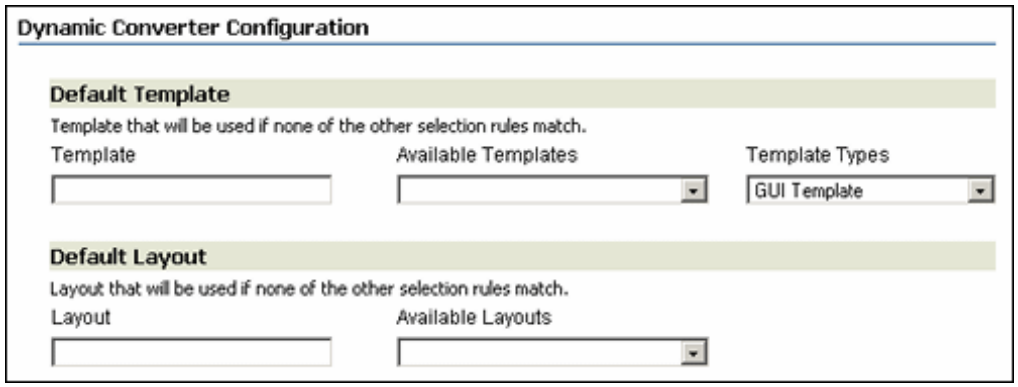
To specify a layout template for a template rule:

1. Open the Dynamic Converter Admin page.
2. Click **Template Selection Rules**.
3. On the Template Selection Rules page, highlight the rule that you would like to specify a layout template for.
4. Enter the content ID for the layout in the **Layout** text box (under the "Template and layout for selected rule" heading). You can also select the layout template from the **Available Layouts** menu.
5. Click **Update** at the bottom of the page.

32.7 Specifying a Default Layout Template

In addition to associating a layout template with a specific template rule, you can also specify a default layout that is applied to all content items that do not match your defined template criteria. You specify the default layout on the Dynamic Converter Configuration page. In Figure 32-5, the template sample titled "default_layout" has been selected.

Figure 32-5 Default Layout Template on Dynamic Converter Configuration Page



To set the default layout template associated with your content items:

1. Open the Dynamic Converter Admin page.
2. Click **Configuration Settings**.
3. On the Dynamic Converter Configuration page, in the **Layout** text box, under the Default Layout heading, enter the content ID for a layout template. You can also choose your layout template from the **Available Layouts** menu.
4. Click **Update** at the bottom of the page to enable your default templates.

32.8 Including Scripts, Images, and CSS in a Layout Template

The layout template that you associate with your content items may include references to other files, such as custom scripts, images, Cascading Styles Sheets (CSS), and more. In fact, if you have a number of script templates that were created in an earlier version of Dynamic Converter, you can copy the Idoc Script tags from those templates and paste them into the new layout template. For more information, see Managing Script Templates .

Identifying the appropriate path to use for an included file can be a challenge because the location of each content item checked into the Content Server may change if its metadata changes (metadata ultimately determines the URL of a content item). As such, you will not know the address of a new content item until it is checked into the Content Server with assigned metadata.

In this type of environment, relative paths create immediate problems. You must use a path that will work from anywhere in the Content Server. See Relative URLs in Templates and Layout Files for a list of solutions.

> **Note:**
>
> To assign a default layout template to your content items, see Setting the Default Template.

33
Managing Script Templates

This chapter describes script templates for dynamic conversion and explains how to use script templates.
This chapter covers the following topics;

- About Script Templates
- Elements
- Indexes
- Macros
- Pragmas
- Setting Script Template Formatting Options
- Breaking Documents by Structure
- Breaking Documents by Content Size
- Using Grids to Navigate Spreadsheet and Database Files

33.1 About Script Templates

Script templates are the text-based conversion templates that were primarily used in earlier versions of Dynamic Converter. They are plain-text files that must be hand-coded with elements, indexes, macros, pragmas, and Idoc Script. You can still use this template format in Dynamic Converter, but Classic HTML Conversion templates (see Managing Conversion Templates) have, for the most part, replaced script templates.

> **Note:**
>
> For more information on Idoc Script, see *Developing with Oracle WebCenter Content*.

The following is the code for a very simple script template:

```
{## unit}{## header}
<html>
<body>
{## /header}
<p>Here is the document you requested.
{## insert element=property.title} by
{## insert element=property.author}</p>

<p>Below is the document itself</p>
{## insert element=body}

{## footer}
</body>
```

```
</html>
{## /footer}{## /unit}
```

The {##unit}, {##/unit}, {##header}, {##/header}, {##footer} and {##/footer} macros can be ignored for the moment. Their purpose is described in Macros.

The remainder of the file is regular HTML code with the exception of three macros in the form {##insert element=xxx}. Dynamic Converter uses this template plus the source file to create its output. To accomplish this, Dynamic Converter reads through the template file, writing it byte for byte to the output file unless character mapping is performed on the template. This continues until the template contains a properly formatted macro. Dynamic Converter reads the macro and executes the macro's command. Usually this means inserting an HTML version of some element from the source file into the output file. Dynamic Converter then continues reading the template and executing macros until the end of the template file is reached.

In the example above, the first {##insert} macro uses the element syntax (described in Insert Element: {## INSERT}) to insert the title of the document. The second macro inserts the author of the document and the third macro inserts the entire body of the document. The resulting HTML might look like this (HTML that is the result of a macro is in **bold**):

```
<html>
<body>
<p>Here is the document you requested.
A Poem by
Phil Boutros</p>

<p>Below is the document itself</p>
<p>Roses are red</p>
<p>Violets are blue</p>
<p>I'm a programmer</p>
<p>and so are you</p>

</body>
</html>
```

33.2 Elements

This section covers the following topics:

- Element Tree
- Leaf Elements
- Repeatable Elements
- Element Definitions

33.2.1 Element Tree

Dynamic Converter uses the concept of an element tree to make various pieces and attributes of the source file individually addressable from within a script template.

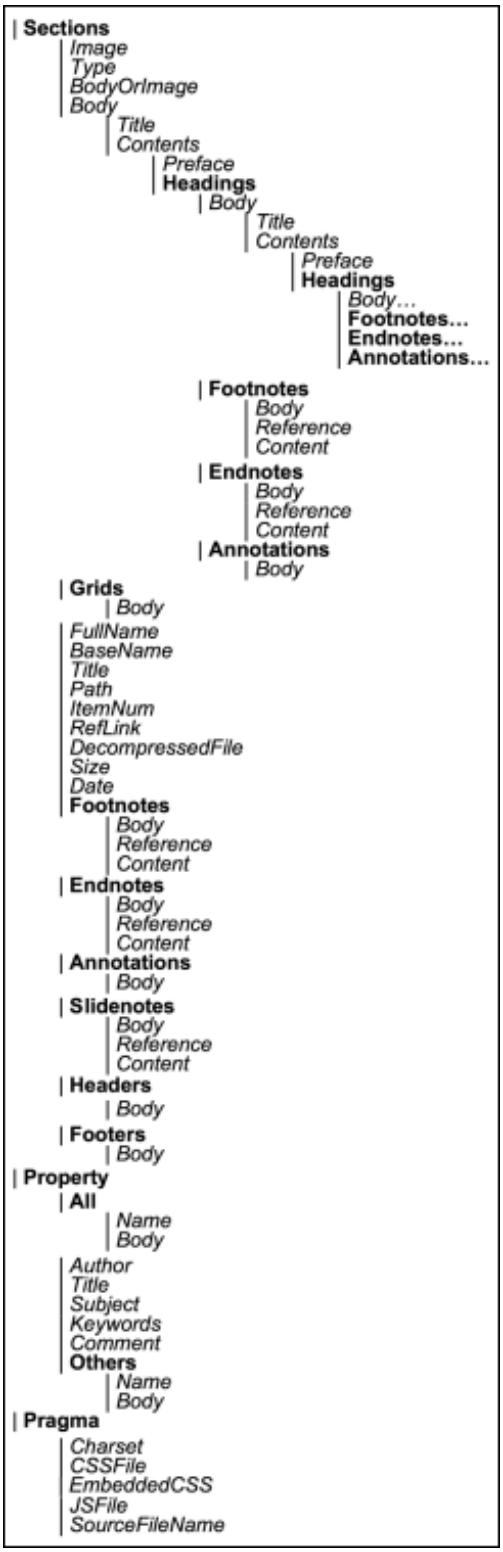
The nodes of the element tree are used to generate a path to a specific element, and a period is used to separate the nodes in this path. For example, the path of the author property of a document is Property.Author.

For convenience, certain nodes in an element path may be skipped because they represent the obvious default behavior. These nodes include the Sections node (Sections.Current.Body.Title is equivalent to Body.Title), and the Body and Contents nodes (Body.Contents.Headings.1.Body is equivalent to Headings.1.Body).

> **Note:**
>
> These nodes may not be skipped if they are the last node in the path (Heading.1.Body is ***not*** equivalent to Headings.1).

There are two types of elements in the element tree: leaf elements and repeatable elements (see Leaf Elementsand Repeatable Elements, respectively).

Figure 33-1 Example of an Element Tree



33.2.2 Leaf Elements

Leaf elements are single identifiable pieces of the source file like the author property (Property.Author) or the preface of the document (Body.Contents.Preface). This type of element is a valid target for inserting, testing and linking using the {##INSERT}, {##F} and {##LINK...} macros. The last node in this type of path must be a valid leaf node in the document tree. Valid leaf nodes are shown in *italics* in the element tree example in Element Tree.

33.2.3 Repeatable Elements

Repeatable elements have multiple instances associated with them, like the footnotes in a document (Sections.1.Footnotes). This type of element may not be directly inserted, tested or linked to but its instances may be looped through using the {##REPEAT} macro. The last node in this type of path must be a valid repeatable node in the document tree. Valid repeatable nodes are shown in **bold** in the element tree example in Element Tree.

Some templates use {##REPEAT} loops to generate one output file per repeatable element. For example, a template may render a presentation file as a group of output files, with one output file for each slide. When an input file contains an exceptionally large number of sections, it is possible for an operating system to run out of file handles. See your operating system's documentation or system administrator to find out how many open file handles are allowed. To avoid this extremely rare problem, set a value for the maxreps attribute of the {##REPEAT} macro or configure the operating system to allow more file handles.

33.2.4 Element Definitions

The following table contains a list of all supported elements and a brief description of each. (For a description of valid values for *x,* see Indexes.)

Element	Type	Description
Property.Author	Leaf	Author property of the source file.
Property.Title	Leaf	Title property of the source file.
Property.Subject	Leaf	Subject property of the source file
Property.Keywords	Leaf	Keywords property of the source file.
Property.Comments	Leaf	Comments property of the source file.
Property.Others	Repeatable	This permits access to all properties not specifically accessible through property elements described above, and includes both the "Name" and the "Body" of the property. Which "Other" properties are supported is file format dependant. Some file formats also allow for additional user definable properties. Only text properties are accessible. Properties such as Yes/No, numeric values, and dates are not supported.
Property.Others.*x*.Name	Leaf	Descriptive name for the property.
Property.Others.*x*.Body	Leaf	Text of the property.
Sheets	Repeatable	See 'Sections' below.
Slides	Repeatable	See 'Sections' below.

Element	Type	Description
Sections	Repeatable	Sections are used to represent the highest level of abstraction within the source file. In general, word processor documents will have only one section, the document itself. Spreadsheets have one section for each sheet or chart. Presentations have one section for each slide. Graphics generally have one section but may have more, as in a multi-page TIFF. For convenience and readability, Sheets and Slides are synonymous with Sections.
Sections.*x*.Body	Leaf	This element represents the main textual area of the source file. For word processing documents, it includes the entire document excluding footnotes, endnotes, headers, footers, and annotations. (Footnote/endnote references are always included automatically in the body. If the template includes footnotes/endnotes, then these references provide a link to the note. Annotation references are not placed in the body unless the template includes annotations, in which case they provide links to the annotations.) For spreadsheets, it includes the entire sheet. For graphics, it includes any text that actually appears as text in the file format.
Sections.*x*.Body.Title	Leaf	For word processing documents, this element is the text marked with the title style. This may be different than the Property.Title. For all other types, this element will be the "name" of the section. For example, if the source file is a spreadsheet, this element will be the name of the sheet as it appears on the spreadsheet application's navigation tabs.
Sections.*x*.Body.Contents	Leaf	For word processing documents, this is the same as Sections.*x*.Body. For all other document types, this is the same as the body minus the title, if a title exists.
Sections.*x*.Body.Contents.Preface	Leaf	Text between the top of the body and the first heading.
Sections.*x*.Body.Contents.Headings	Repeatable	Headings are labels in a word processor document inserted by the author to give a document structure. See Breaking Documents by Structure for more information on headings. Dynamic Converter reads this structure and, through the use of the Headings element, allows you to access it.
Sections.*x*.Body.Contents.Headings.*x*.Body.	Leaf with Leaves and Repeatables below	Under each heading, the structure of a complete document from Body down is repeated. See Breaking Documents by Structure for a clearer picture of how these elements map to parts of a document.
Sections.*x*.Body.Contents.Headings.*x*.Footnotes	Repeatable with Leaves below	Only footnotes contained in this heading.
Sections.*x*.Body.Contents.Headings.*x*.Endnotes	Repeatable with Leaves below	Only endnotes contained in this heading.
Sections.*x*.Body.Contents.Headings.*x*.Annotations	Repeatable with Leaves below	Only annotations contained in this heading.

Element	Type	Description
Sections.*x*.Grids	Repeatable	Only valid for spreadsheet and database formats. This permits access to the "grids" inside a section or sheet of a spreadsheet or database file.
Sections.*x*.Grids.*x*.Body	Repeatable	Only valid for spreadsheet and database formats. This permits access to the "grids" inside a section or sheet of a spreadsheet or database file.
Sections.*x*.Image	Leaf	This element represents a graphic image of the content of the section. It is valid only for bitmap, drawing, chart and presentation sections.
Sections.*x*.BodyOrImage	Leaf	This element exists to make it easy to build templates that handle a range of section types. In word processing documents, spreadsheets and database sections, BodyOrImage is synonymous with Body. In bitmap, drawing, chart and presentation sections, BodyOrImage is synonymous with Image.
Sections.*x*.Title	Leaf	Same as Sections.*x*.Body.Title. For word processing documents, this element is the text marked with the title style. This may be different than the Property.Title. For all other types, this element will be the "name" of the section. For example, if the source file is a spreadsheet, this element will be the name of the sheet as it appears on the spreadsheet application's navigation tabs.
Sections.*x*.Type	Leaf	This element exists only for query purposes. It is valid only at the ELEMENT of a {##IF...} macro. This element is normally used only for query purposes, but it may be inserted as well. See Conditional: {## IF...}_ {## ELSEIF...}_ and {## ELSE} for further details on how to use this in an {##IF} macro.
Sections.*x*.Footnotes	Repeatable	All footnotes.
Sections.*x*.Footnotes.*x*.Body	Leaf	The complete footnote reference and content text.
Sections.*x*.Footnotes.*x*.Reference	Leaf	The reference number for the footnote.
Sections.*x*.Footnotes.*x*.Content	Leaf	The content text for the footnote.
Sections.*x*.Footnotes	Repeatable	All footnotes.
Sections.*x*.Endnotes.*x*.Body	Repeatable with Leaves below	The complete endnote reference and content text.
Sections.*x*.Endnotes.*x*.Reference	Repeatable with Leaves below	The reference number for the endnote.
Sections.*x*.Endnotes.*x*.Content	Repeatable with Leaves below	The content text for the endnote.
Sections.*x*.Annotations	Repeatable	All annotations.
Sections.*x*.Annotations.x.Body	Leaf	The complete annotation reference and content text.
Sections.*x*.Annotations.x.Reference	Leaf	The reference text for the annotation.
Sections.*x*.Annotations.*x*.Content	Leaf	The content text for the annotation.

Element	Type	Description
Sections.*x*.Slidenotes	Repeatable	All slide notes. Please note that converting the slide notes will slow down the conversion process for PowerPoint files.
Sections.*x*.Slidenotes.*x*.Body	Leaf	The notes for the current slide. It is recommended that you write slide notes at the end of the output file for performance reasons (PowerPoint files keep slide notes at the end of the file, not next to each slide). Not doing so will slow conversion, as the technology will be forced to perform excessive seeking in the input file.
Sections.*x*.Headers	Repeatable	All headers.
Sections.*x*.Headers.*x*.Body	Leaf	Text of the header.
Sections.*x*.Footers	Repeatable	All footers.
Sections.*x*.Footers.*x*.Body	Leaf	Text of the footer.
Pragma.Charset	Leaf	The HTML text string associated with the character set of the characters that Dynamic Converter is generating. In order for Dynamic Converter to correctly code the character set into the HTML it generates, all templates should include a META tag that uses the {##INSERT} macro as follows. <META HTTP-EQUIV="Content-Type" CONTENT="text/html; charset={## INSERT ELEMENT=pragma.charset}"> If the template does not include this line, the user will have to manually select the correct character set in their browser.
Pragma.SourceFileName	Leaf	The name of the source document being converted. Note that this does NOT include the path name.

Element	Type	Description

Pragma.CSSFile	Leaf	This element is used to insert the name of the Cascading Style Sheet (CSS) file into HTML documents. This name is typically used in conjunction with an HTML <LINK> tag to reference styles contained in the CSS file generated by Dynamic Converter.
		When used with the {##INSERT} macro, this pragma will generate the URL of the CSS file that is created. This macro must be used with {##INSERT} inside every template file that inserts contents of the source file and when the selected HTML flavor supports CSS. The CSS file will only be created if the selected HTML flavor supports CSS.
		When used with the {##IF} macro, the conditional will be true if the selected HTML flavor supports Cascading Style Sheets or not.
		If CSS is required for the output, {##IF element=pragma.embeddedcss} or {##IF element=pragma.cssfile} must be used. However, Dynamic Converter does not differentiate between the two, as the choice of using embedded CSS vs. external CSS is your decision and you may even wish to mix the two in the output.
		An example of how to use this pragma that works when exporting either CSS or non-CSS flavors of HTML would be as follows:
		`{## IF ELEMENT=Pragma.CSSFile}`
		`<LINK REL=STYLESHEET`
		`HREF="{## INSERT`
		`ELEMENT=Pragma.CSSFile}">`
		`</LINK>`
		`{## /IF}`

Pragma.EmbeddedCSS	Leaf	This element is used to insert CSS style definitions in a single block in the <HEAD> of the document. When used with the {##INSERT} macro, this pragma will insert the block of CSS style definitions needed for use later in the file. This macro must be used inside every output HTML file where {##INSERT} is used to insert document content. When used with the {##IF} macro, the conditional will be true if the selected HTML flavor supports CSS. If CSS is required for the output, {##IF element=pragma.embeddedcss} or {##IF element=pragma.cssfile} must be used. However, Dynamic Converter does not differentiate between the two, as the choice of using embedded CSS vs. external CSS is your decision and you may even wish to mix the two in the output. If a style is used anywhere in the input document, that style will show up in the embedded CSS generated for all the output HTML files generated for the input file. Consider a template that splits its output into multiple HTML files. In this example, the input file contains the "MyStyle" style. It does not matter if during the conversion only one output HTML file actually references the "MyStyle" style. The "MyStyle" style definition will still show up in the embedded CSS for all the output files, including those files that never reference this style.

Element	Type	Description
Pragma.JsFile	Leaf	This element is used to insert the name of the JavaScript file into HTML documents. This name is typically used in conjunction with an HTML <SCRIPT> tag to reference JavaScript contained in the `.js` file generated by HTML Export. When used with the {##INSERT} macro, this pragma will generate the URL of the JavaScript file that is created. This macro must be used with {##NSERT} inside every template file that inserts contents of the source file when: • The selected HTML flavor supports JavaScript. • The javaScriptTabs option has been set to true. The JavaScript file will only be created if the selected HTML flavor supports JavaScript. When used with the {##IF} macro, the conditional will depend upon whether the selected HTML flavor supports JavaScript or not.

33.3 Indexes

Repeatable nodes have an associated index variable that has a current value at any given time in the export process. For elements that contain repeatable nodes as part of their paths, the instance of the repeatable element must be specified by using a number or one of the index variable keywords.

This section covers the following topics:

- Index Variable Keywords
- Example: Creating a Set of HTML Files for Each Slide in a Presentation

33.3.1 Index Variable Keywords

The possible values for this index (referred to as 'x' in element definitions (see Element Definitions) are as follows:

- Whole Number
- Current, Next, Previous, First, and Last
- Up, Down, Left, and Right

33.3.1.1 Whole Number

For numeric values, the number is simply inserted as another node in the path.

> **Note:**
>
> Dynamic Converter indexes begin counting with 1 (not 0).

For example, *Slides.1.Image* references the first slide in a presentation and *Footnotes.2.Body* references the second footnote in a document.

If it cannot be guaranteed that elements are within the document which the template is applied on, they should not be explicitly referenced. For example, referencing *Sections.4.Body* may result in unexpected behavior in documents that have fewer than four sections.

Requesting a non-existent element will not cause an error in Dynamic Converter. The insertion will just be ignored. However, if other HTML surrounding the insertion depends on the results of the insert, the output may be invalid HTML.

33.3.1.2 Current, Next, Previous, First, and Last

The 'current', 'next', 'previous', 'first', and 'last' keywords are fairly self-explanatory. When the script template is processed, these variables are replaced with the appropriate index value. For example, *Slides.Current.Image* references the current slide and *Slides.Next.Image* refers to the next slide.

'Next' and 'previous' do not change the value of the index, as was the case in earlier versions of Dynamic Converter. As a result, the only places where the index is changed are inside of a {##REPEAT} loop and as the result of a {##LINK} statement.

{## REPEAT…}

The initial value of the index variable for any given repeatable element typically is 1. For {##REPEAT} loops, the index is incremented with each iteration. Termination of a {##REPEAT} loop resets the counter to its initial value. Actually, it is more accurate to say that the scope of the index is the repeat loop.

The following template fragment uses `current` in a repeat loop, which outputs all the footnotes in the source file:

```
{## REPEAT element=footnotes}
{## INSERT element=footnotes.current.body}
{## /REPEAT}
```

When a template containing a repeat statement is the target of a {##link} statement that specifies the element to be used as the repeat element, the initial value of the index will be determined by the {##LINK} processing.

{## LINK…}

The {##LINK} statement does not affect the index variable in the context of the current template. The {##LINK} statement can only affect index variables when both an element and a template are specified. In this case only the index variables in the target for the specified element are affected.

If the element specified in the {##LINK} contains a next or previous keyword, the value of current in the target file will be affected. The initial value of current in the target will be the value of (current in the source)+1 for next. Similarly, previous has the effect of decrementing the value of current.

The following example uses a single template file and the `{##link}` macro to create a set of HTML files, one for each slide in a presentation. The `{##link}` does the dual job of driving the generation of the HTML files and providing a "next" link for navigation. Notice the use of the `next` keyword in the `{##if}` macro that checks to see if there is a next slide:

```
{## unit}
<html>
<body>
```

```
<!-- insert the current slide -->
{## insert element=slides.current.image width=300}
<hr />
<!-- Is there a next slide? -->
{## if element=slides.next.image}
 <!-- If yes, generate a URL to an HTML file containing
 the next slide. The HTML file is generated using
 the current template (because there is no template
 attribute). While generating the new HTML file, the
 value of the index on slides will be its current
 value plus 1 once control returns to this template,
 the value of the index on slides is unchanged. -->
 <p><a href="{## link element=
 slides.next.image}">Next</a></p>
{## else}
 <!-- If no, create a link to the HTML containing the
 first slide. -->
 <p><a href="{## link element=
 slides.1.image}">First</a></p>
{## /if}
</body>
</html>
{## /unit}
```

33.3.1.3 Up, Down, Left, and Right

In addition to the Current_ Next_ Previous_ First_ and Last index variable keywords, repeatable grid elements have four additional keywords:

- Up
- Down
- Left
- Right

These keywords may only appear immediately after the Grids node in the document tree. For example, *Grids.Up.Body* is legal, but *Sections.Left.Grids.1.Body* is not. Use of these keywords is otherwise self-explanatory.

Note, too, that individual grids are only addressable relative to each other. In other words, while it is possible to specify the "up" grid, it is not possible to arbitrarily specify a grid directly (that is, "5, 7").

33.3.2 Example: Creating a Set of HTML Files for Each Slide in a Presentation

The following example uses a single script template file and the {##LINK...} macro to create a set of HTML files, one for each slide in a presentation. The {##LINK...} does the dual job of driving the generation of the HTML files and providing a "next" link for navigation. Notice the use of the Next keyword in the {##IF...} macro that checks to see if there is a next slide.

```
<html>
<body>
<!-- Insert the current slide -->
{## INSERT ELEMENT=Slides.Current.Image WIDTH=300}
<hr />
```

```
<!-- Is there a next slide? -->
{## IF ELEMENT=Slides.Next.Image}
<!-- If yes, generate a URL to an HTML file containing the next slide. The HTML file
is generated using the current template (because there is no TEMPLATE attribute).
While generating the new HTML file, the value of the index on Slides is its current
value plus 1 once control returns to this template, the value of the index on Slides
is unchanged. -->
<p><a href="{## LINK ELEMENT=Slides.Next.Image}">Next</a></p>
{## ELSE}
<!-- If no, create a link to the HTML containing the first slide. -->
<p><a href="{## LINK ELEMENT=Slides.1.Image}">First</a></p>
{## /IF}
</body>
</html>
```

33.4 Macros

This section covers the following topics:

- About Macros
- Units: {## UNIT}_ {## HEADER}_ and {## FOOTER}
- Insert Element: {## INSERT}
- Conditional: {## IF...}_ {## ELSEIF...}_ and {## ELSE}
- Loop: {## REPEAT}
- Linking With Structured Breaking: {## LINK}
- Linking With Content Size Breaking: {## ANCHOR}
- Comment Put in the Output File: {## IGNORE}
- Comment Not Put in the Output File: {## COMMENT}
- Including Other Templates: {## INCLUDE}
- Setting Options Within the Template: {## OPTION}
- Copying Files: {## COPY}
- Deprecated Template Macros

33.4.1 About Macros

Macros are commands to Dynamic Converter within script templates. Despite their casual similarity to HTML tags, they are not bound by any of the rules that tags would usually follow inside an HTML file. Macros may appear anywhere in the script template file, except inside another macro.

In the documentation and examples, the pieces of a macro are always shown delimited by spaces. However, semicolons may also delimit them. This option was added to accommodate certain HTML editors. In certain editors, URLs entered into dialog boxes may not have non-quoted spaces. This made it difficult or impossible to use the {##LINK} macro in these situations.

For example, `{##INSERT ELEMENT=Sections.1.Body}` may also be written as `{##;INSERT;ELEMENT=Sections.1.Body}`.

Note that template macro string parameters and options support sprintf style escaped characters. This means that characters such as \x22, \r and %%are supported. Also note that most template attribute values may be quoted. The exception is template element strings, which may not be quoted at this time.

For example:

```
{## ANCHOR aref="next" format="<a href=\"%url\">Next</a><br/>\r\n"}
```

33.4.2 Units: {## UNIT}, {## HEADER}, and {## FOOTER}

If a template file is going to make use of the {##UNIT} macro at all, this macro must be the first macro in the template file. It delimits the beginning and end of each unit. Unit boundaries are used when determining where to break the document when breaking based on content size (see Breaking Documents by Content Size).

A unit consists of a header, a footer (both of which are optional), and a body (which may be empty). To ensure that the header is the first item in the template and the footer is the last item, text between the {##UNIT} tag and the {##HEADER} tag will be ignored, as will text between the {##/FOOTER} tag and the {##/UNIT} tag, including whitespace. The header and footer of a unit will be output in every page containing that unit, enclosing that portion of the unit's body that is able to fit in a particular page. The entire template is a unit that may contain additional units.

Syntax

```
{## UNIT [BREAK]}
 [{##HEADER}
 any HTML
 {##/HEADER}]

 any HTML

 [{##FOOTER}
 any HTML
 {##/FOOTER}]
{## /UNIT}
Attributes
BREAK
```

Attribute	Description

BREAK	This optional attribute forces a page break before inserting the unit contents unless doing so would cause the body of the first page to be empty. One situation where this attribute would be useful would be to force a page break between each section of a document, perhaps to get one presentation slide per page.
	The {##UNIT} macro and its BREAK attribute are ignored when SCCOPT_EX_PAGESIZEpagesize is set to zero.
	It is sometimes important to make sure that a break does not occur in the midst of text that is intended to be on the same page. To prevent breaks like this from occurring, enclose the text that should be kept on the same page inside a nested {##UNIT}{## HEADER} pair. For example, to prevent a page break from occurring while a link is being created, the template author might write something like the following:
	`{## unit}{## header}`
	`<a href="{## link element=sections.current.body}">Link</a>`
	`{## /header}{## /unit}`

33.4.3 Insert Element: {## INSERT}

This macro inserts an element of the source file into the output file at the current location.

Syntax

```
{## INSERT [ELEMENT=element [WIDTH=width] [HEIGHT=height] [SUPPRESS=suppress]
[TRUNCATE=truncate]] |[NUMBER=number] [URLENCODE]}
```

Attribute	Description
ELEMENT	This attribute describes which part of the source file should be placed in the output file at the location of the macro. See Element Definitionsfor the possible values for this attribute. If the value of this attribute is not in the element tree, Dynamic Converter considers it to be a custom element and the EX_CALLBACK_ID_PROCESSELEMENTSTR callback is called. Example: {##INSERT ELEMENT=Sections.1.Body}
WIDTH	This optional attribute defines the width in pixels of the element being inserted. It is currently only valid for the Image element. If the WIDTH attribute is not present but the HEIGHT attribute is, the width of the image is calculated automatically based on the shape of the element. If neither the WIDTH and HEIGHT attributes are present, the image's original dimensions are used. If the image's original dimensions are unknown, the defaults assume a HEIGHT and WIDTH of 200. Example: {##INSERT ELEMENT=Slides.1.Image WIDTH=400}
HEIGHT	This optional attribute defines the height in pixels of the element being inserted. It is currently only valid for the Image element. If the HEIGHT attribute is not present, but the WIDTH attribute is, the height of the image is calculated automatically based on the shape of the element. Example: {##INSERT ELEMENT=Slides.1.Image HEIGHT=400}

Attribute	Description

SUPPRESS	This optional attribute allows certain things to be suppressed from the output. This is very useful if elements need to be inserted in contexts where HTML is not appropriate, such as passing information to Java applets, ActiveX controls, or populating parts of a form. Possible values are as follows:
	TAGS: All HTML tags are suppressed from the output of the element, however the text may still contain HTML character codes like " or {
	For non-embedded graphics such as presentations and graphic files, the URL of the converted graphic will not be suppressed. The <img> tag that would normally surround the URL is suppressed, however.
	For embedded graphics such as those found in word processing sections and spread sheets, both the URL and the <IMG> tag are suppressed. Because there would be no way to access the resulting converted embedded graphic, conversion of the graphic is not done.
	Example:
	`<form method="POST">`
	`<input type="text" size="20" name="Author"`
	`value="{## INSERT ELEMENT=Property.Author SUPPRESS=TAGS}">`
	`</form>`
	
	BOOKMARKS: Turns off all bookmarks in the inserted section. Bookmarks automatically precede many inserted elements so that other template elements may link to them. SUPPRESS=BOOKMARKS is provided to prevent problems with nested <a> tags. Note that this represents a subset of the suppression behavior provided by SUPPRESS=TAGS.
	INVALIDXMLTAGCHARS: Drops from the output all characters that are not allowed in XML tag names. This is designed to allow template authors to {##INSERT} custom document property names inside angle brackets ("<" and ">") to create XML tags. Most characters in Unicode and its subset character sets may be used as part of XML tag names. Illegal tag characters include "control" characters such as line feed and carriage return. In addition there are special rules for what characters can be the first character in a tag name.
	Example:
	`{## REPEAT Sections.Property.Others}`
	`<{## INSERT ELEMENT=Property.Others.Current.Name`
	`SUPPRESS=InvalidXMLTagChars}>`
	`<{## INSERT ELEMENT=Property.Others.Current.Body`
	`SUPPRESS=InvalidXMLTagChars}>`
	`</{## INSERT ELEMENT=Property.Others.Current.Name`
	`SUPPRESS=InvalidXMLTagChars}>`
	`{/## REPEAT}`
	
	produces something similar to the following:
	<MyProperty>PropertyValue</MyProperty>

Attribute	Description
TRUNCATE	When set, this attribute forces a maximum length in characters for the inserted element. This allows elements to be truncated rather than broken across pages when the page size option is in use. Truncated elements will end with the truncation identifier which is "…" (three periods). All elements that have a truncate value will be no more than the specified number of characters in length including the length of the truncation identifier. In Dynamic Converter, elements are inserted in their entirety if no truncation size is specified. The value of this attribute must be greater than or equal to five characters. An example of a situation where element truncation is useful is to limit the size of entries when building a table of contents. The TRUNCATE attribute implies suppression of tags for the insert. It also auto applies the no source formatting option for the insert. Note that the TRUNCATE attribute cannot be used with custom elements, because the custom element definition precludes the existence of any other attributes to {##INSERT}. The TRUNCATE attribute has three special aspects to its behavior when grids are being inserted: When truncation is in effect, the truncation size refers to the number of characters of content in each cell, not the number of characters in the grid as a whole. While truncation normally causes all markup tags to be suppressed, when grids are in use, the table tags are retained (assuming that the output flavor supports tables). Users are reminded that only one grid size may be selected for each spreadsheet sheet or database inserted. The size of the grid will be based in part on the TRUNCATE value if one or both the grid dimensions are not specified and the SCCOPT_EX_PAGESIZE option is in use. In this situation, if a grid from a single sheet is inserted in more than one place in the template, and there are differing TRUNCATE values, then the grid dimensions will be based on the largest TRUNCATE value specified.

Attribute	Description

NUMBER	This attribute allows the developer to retrieve the total instance count or the current index value of any repeatable element. This can be very useful for writing JavaScript, BasicScript, etc. Two special keywords do not appear in the element tree but can be used as nodes in the following special case.
	Count and CountB0: When appended to a repeating element and used with the NUMBER attribute, these nodes allow the developer to insert a text representation of the number of instances of the given repeatable element. Count gives the count assuming the first index is 1 and CountB0 gives it assuming the first index is 0.
	Example: If a presentation has three slides, the template fragment,
	`<P>{## INSERT NUMBER=Slides.Count}`
	`<P>{## INSERT NUMBER=Slides.CountB0}`
	produces the following text:
	`<P>3`
	`<P>2`
	Value and ValueB0: When appended to a repeating element and used with the NUMBER attribute, these nodes allow the developer to insert a text representation of the current value of the index of the given repeatable element. Value gives the count assuming the first index is 1 and ValueB0 gives it assuming the first index is 0.
	Example: If the current value of the index on Slides is 2, the template fragment,
	`<P>{## INSERT NUMBER=Slides.Current.Value}`
	`<P>{## INSERT NUMBER=Slides.Current.ValueB0}`
	Produces the following text:
	`<P>2`
	`<P>1`

URLENCODE	This optional attribute causes the inserted element to be URL encoded. As such, it is ignored unless it is specified as part of an insert that contains a file name. The following elements may be URL encoded: • pragma.sourcefilename • pragma.cssfile • pragma.embeddedcss • pragma.jsfile In addition, the following elements will be URL encoded when the section type is "Archive" or "AR": • sections.x.fullname • sections.x.basename • sections.x.body • sections.x.title • sections.x.reflink For all other {##INSERT} tags, this attribute is ignored. As such, you should note that Dynamic Converter does not modify any URLs coming out of the input documents being converted. These URLs continue to be passed through as is. This attribute is also ignored if the URL was created using the EX_CALLBACK_ID_CREATENEWFILE callback. Such URLs are assumed to already be URL-encoded.

Inserting Properties

Because of the special ways that properties are used in documents, property strings are inserted into the output HTML a little differently than the way other {##INSERT} macros work.

The property is always inserted as if the SCCOPT_NO_SOURCEFORMATTING option were set. This prevents formatting characters such as new lines from interfering with the property strings.

The property is always inserted as if the script template specified `Suppress=Tags`. This provides you with maximum control over how property strings are presented.

33.4.4 Conditional: {## IF...}, {## ELSEIF...}, and {## ELSE}

This macro allows an area of the script template to be used based on information about an element of the source file.

Syntax

```
{## IF ELEMENT=element [CONDITION=Exists|NotExists]
[VALUE=value]}
 any HTML
{## /IF}
```

or

```
{## IF ELEMENT=element [[CONDITION=Exists|NotExists] |
[VALUE=value]]}
 any HTML
{## ELSE}
 any HTML
{## /IF}
```

or

```
{## IF ELEMENT=element [[CONDITION=Exists|NotExists] |
[VALUE=value]]}
 any HTML
{## ELSEIF ELEMENT=element [[CONDITION=Exists|NotExists] |
[VALUE=value]]}}
 any HTML
{## ELSE}
 any HTML
{## /IF}
```

> **Note:**
>
> Multiple {##ELSEIF} statements may be used after {##IF}. In addition, {##ELSE} is not required when using {##ELSEIF}.

Attribute	Description
ELEMENT	This attribute describes which part of the source file should be tested. See Element Definitions for the possible values for this attribute. If neither the CONDITION nor VALUE attribute exists, the element is tested for existence.

Attribute	Description
CONDITION	Defines the condition the element is tested for, possible values are EXISTS and NOTEXISTS.

VALUE	Defines the values the element should be tested against. The VALUE attribute is currently valid only for the Sections.x.Type element for testing of the type of a section of the source file.
	Possible values include:
	• ar =archive
	• bm =bitmap
	• ch =chart
	• db =database
	• dr =drawing
	• mm =multimedia
	• pr =presentation
	• ss =spreadsheet
	• wp =word processing document
	Examples:
	`{## if element=property.comment}`
	` <p><b>Comment property exists</b></p>`
	`{## else}`
	` <p><i>Comment property does not exist</i></p>`
	`{## /if}`
	`{## if element=sections.1.type value=wp}`
	` <p><b>The source file is a word processor file</b></p>`
	`{## /if}`
	`{## if element=sections.1.type value=ss}`
	` <p>Spreadsheet</p>`
	`{## elseif element=sections.1.type value=ar}`
	` <p>Archive</p>`
	`{## elseif element=sections.1.type value=ch}`
	` <p>Chart</p>`
	`{## else}`
	` <p>Not ss, ar, or ch</p>`
	`{## /if}`
	`{## if element=sections.current.type value=pr`
	` condition=notexists}`
	` <p>We can do something here for all document types`
	` other than presentations.</p>`
	`{## else}`
	` <p>This is used only for presentations.</p>`
	`{## /if}`

33.4.5 Loop: {## REPEAT}

This command allows an area of the script template to be repeated, once for each occurrence of an element.

Syntax

```
{## REPEAT ELEMENT=element [MAXREPS=maxreps] [SORT=sort]}
 any HTML
{## /REPEAT}
```

Attribute	Description

ELEMENT	This attribute describes what part of the source file should be repeated on. It must be a repeatable element. See Element Definitions for the possible values for this attribute.
	Any HTML may be defined between the {##REPEAT... }macro and its closing {##/REPEAT} macro. This HTML is repeated once for each instance for the element specified. In addition, the word Current may be used in any other {##}tag as the element-index of the element being repeated. For instance, the following HTML in the template will produce a list of the footnotes in the document.
	Example:
	`<HTML>`
	`<BODY>`
	`<P>Here are the footnotes`
	`{## REPEAT ELEMENT=Footnotes}`
	`<P>{## INSERT ELEMENT=Footnotes.Current.Body}`
	`{## /REP}`
	`<P>No more footnotes`
	`</BODY>`
	`</HTML>`
	
	Similarly, the following HTML in the template will insert the names of all the items in an archive:
	`{## repeat element=sections}`
	`{##insert element=sections.current.fullname}`
	`{## /repeat}`

MAXREPS	This attribute limits the total number of loops the repeat statement may make to the value specified. It is useful for preventing exceptionally large documents from producing an unwieldy amount of output.
SORT	This optional attribute defines whether to sort the output or not. This attribute is ignored if the input file is not an archive file of arctype file. All sorts are done based on the character encoding of the values in the input file. The sorts are also case insensitive at this time. Valid values of the sort attribute are: • **fullname**: sort by Sections.Current.FullName • **basename**: sort by Sections.Current.BaseName • **none**: no sorting is done. This is the default.

33.4.6 Linking With Structured Breaking: {## LINK}

This macro generates a relative URL to a piece of the document produced by Dynamic Converter. Normally this URL would then be encapsulated by the template with HTML anchor tags to create a link. {##LINK} is particularly powerful when used within a {##REPEAT} loop.

Syntax

```
{## LINK ELEMENT=element [TOP]}
```

or

```
{## LINK TEMPLATE=template}
```

or

```
{## LINK ELEMENT=element TEMPLATE=template [TOP]}
```

Attribute	Description
ELEMENT	Defines the element that is the target for the link. The URL that the {##LINK...} macro generates will point to the first instance of this element in the output file. If this attribute is not present, the resulting URL will link to any output file that was produced with the specified script template. If such a file does not exist, the specified script template is used to generate a file. Remember that each element has one or more index values, some of which may be variables. An example of this type of index variable is the "current" in Sections.Current.Body. Use of {##LINK} affects the value of those index variables, which may cause subtle side effects in the behavior of the linked template file. For a description of how {##LINK} affects the index of inserted elements more information, see Indexes.
TEMPLATE	The name of a template file which must exist in the same directory as the original template file. If this attribute is not present, the current template will be used. If an element was specified in the {##LINK}, then the template must contain a {##INSERT} statement using that element. It is important to note that while the template language is normally case-insensitive, the case of the template file names specified here is important. The file name specified for the template is passed as is to the operating system. On operating systems such as UNIX, if the wrong case is given for the template file name, the template file will not be found and an error will be returned.
TOP	This attribute is only meaningful if an element is specified in the {##LINK} command. When this attribute exists, the generated URL will not contain a bookmark, and therefore the resulting link will always jump to the top of the HTML file containing the specified element. This is useful if the top of the script template has navigation or other information that the developer would like the user to see.

33.4.6.1 {## LINK} Usage Scenarios

Using the first syntax shown at the beginning of this section, a URL for the element bookmark is inserted in the document. Normally this syntax is used to create intradocument links to aid navigation. An example would be creating a link to the next section of the document.

In the second syntax, a URL is created to an output file generated by the specified template. This template is run on the same source document, but may extract different parts of the document. Normally, in this syntax, the "main" template contains a link to a second HTML file. This second file is generated using the template specified by the {##LINK} command and contains other document elements. As an example, the "main" template could produce a file containing the body of the document and a link to the second HTML file, which contains the footnotes and endnotes.

The third and most powerful syntax also produces the URL of a file generated by the specified template. This template is then expected to contain an insertion of the specified element. Normally this syntax is used with repeatable elements. It allows the author to generate multiple output files with sequential pieces of the document. As such it provides a way to break large documents up into smaller, more readable pieces. An example of where this syntax would be used is a template that generates a "table of contents" in one HTML file (perhaps a separate HTML frame). The entries in the table are then links to other HTML files generated by different templates.

Note that a {##LINK} statement which specifies a template does not always result in a new file being created. New files are only created if the target of the link does not exist yet. So if for example two {##LINK} statements specify the same element and template, only one HTML file is produced and the same URL will be used by both {##LINK} statements.

33.4.6.2 {## LINK} Archive File Example

The following template generates a list of links to all the extracted and converted files from the source archive file (represented by decompressedFile in the following example):

```
{## repeat element=sections}
 <p><a href="{## link element=sections.current.decompressedFile}">
 {##insert Element=sections.current.fullname}</a></p>
{## /repeat}
```

33.4.6.3 {## LINK} Presentation File Example

The following example (`template.htm`) uses the first syntax to generate a set of HTML files, one for each slide in a presentation. Each slide will include links to the previous and next slides and the first slide. Note the use of {##IF} macros so the first and last slides do not have Previous and Next links respectively:

```
template.htm
 <html>
 <body>
 {##insert element=slides.current.image width=300}
 <hr />
 {##if element=slides.previous.image}
 <p><a href={## link element=slides.previous.image}>
 previous</a></p>
 {##/if}
 {##if element=slides.next.image}
 <p><a href={## link element=
 slides.next.image}>Next</a></p>
 {##/if}
 </body>
 </html>
```

Due to the side effects of {##LINK} using the element attribute, there can be some confusion over what values "current," "previous" and "next" have when each {##LINK} is processed. To better illustrate how this template works, consider running it on a presentation that contains three slides:

First Output File

Because no template is specified in the {##LINK} statements, `template.htm` is (re)used as the template for all {##LINK} statements. For the first slide, nothing interesting happens until `slides.next` is encountered. Because `slides.current` is 1 in this case, `slides.next` refers to `slides.2` and the {##LINK} is performed on `slides.2.image`. This {##LINK} fills in the anchor tag with the URL for the output file containing the second slide. Because no file containing `slides.2` exists, {##LINK} opens a new file.

Second Output File

For the second slide the template is rerun. `slides.current` now refers to `slides.2`, `slides.previous` refers to `slides.1` and `slides.next` refers to `slides.3`. The {##INSERT} statement will insert the second slide.

The {##IF} statement referring to `slides.previous` succeeds. Because the file containing `slides.1` already exists, no additional file is created. The anchor tag will be filled in with the URL for the first output file.

The {##IF} statement referring to `slides.next` also succeeds and the anchor tag will be filled in with the URL for the output file containing the third slide. Because no file containing `slides.3` exists, {##LINK} opens a new file.

Third Output File

For the third slide the template is rerun. `slides.current` now refers to `slides.3` and `slides.previous` refers to `slides.2`. `slides.next` refers to `slides.4`, which does not exist. The {##INSERT} statement will insert the third slide.

The {##IF} statement referring to `slides.previous` succeeds. Because the file containing `slides.2` already exists, no additional file is created. The anchor tag will be filled in with the URL for the second output file.

The {##IF} statement referring to `slides.next` fails. At this point processing is essentially complete.

33.4.7 Linking With Content Size Breaking: {## ANCHOR}

This macro generates a relative URL to a piece of the document produced by Dynamic Converter when doing document breaking based on content size.

Syntax

```
{## ANCHOR AREF=type [STEP=stepval] FORMAT="anchorfmt" [ALTLINK="element"]
[ALTTEXT="text"]}
```

Attribute	Description
AREF	Indicates the relation of the target of the link to the current file. Allowable values for this attribute are: • **nsertStart**: links to first page of the inserted element • **InsertEnd**: links to last page of the inserted element • **Next**: links to next page in the inserted element • **Prev**: links to previous page in the inserted element • **FirstFile**: links to first page created for the entire document • **LastFile**: links to last page created for the entire document
STEP	This attribute is used to insert a link to "fast forward/rewind" through the output pages. This attribute may only be used if AREF is "next" or "prev." It is specified as a non-zero positive integer. For example, to insert a link to skip ahead five pages in a document, the following statement could be used: `{## unit aref="next" step="5" format="<p><a href=\"%url\">Next</a></p>"}` If not specified, the default value of the STEP attribute is one (1), which corresponds to the next/previous page. This attribute has no meaning when `aref` equals "insertstart," "insertend," "firstfile," or "lastfile."

Attribute	Description
FORMAT	This is a sprintf style format string specifying the text to output as the link. Dynamic Converter replaces the %url format specifier with the target URL into the format string. For example: `{## anchor aref="next" format="<a href=\"%url\">Next</a> \r\n"}`
ALTLINK	An attribute used to specify the target of the anchor if it cannot be resolved based on the anchor type. For example, the final file of a breakable element has no "next" file, and thus would resolve to nothing. However, if the altlink attribute is specified, the anchor will be generated using a URL to the first file found containing the specified element. Note that no EX_CALLBACK_ID_ALTLINK callback will be made if an EX_CALLBACK_ID_ALTLINK attribute is specified in the {##ANCHOR} statement. For example: `{## anchor aref=next format="<a href=\"%url\">Next</a>" altlink=headings.next.body}`
ALTTEXT	Text to be output if the anchor cannot be resolved. If this attribute is not specified, no text will be output if the anchor target does not exist. For example: {## anchor aref=next format="Next" alttext="Next"}

33.4.8 Comment Put in the Output File: {## IGNORE}

This macro causes {##}statements in an area of the template file to be ignored by the template parser. Any text between the {##IGNORE} and {##/IGNORE} tags will be written to the output file as-is. This macro allows {##}statements in an area of the template to be commented out for debugging purposes, or to actually write out the text of another {##}macro. However, the browser will parse any HTML tags inside the ignored block and the text will be formatted accordingly. This macro can ignore all {##}macros except for an {##/IGNORE} macro. No escape sequence has been implemented for this purpose. As a result, {##IGNORE} statements cannot be nested. If they are nested, a run time template parser error will occur.

Syntax

```
{## IGNORE}
 any HTML or other {##}macros
{## /IGNORE}
```

> **Note:**
>
> To fully comment out a section of the script template, surround the ##IGNORE statements with HTML comments, for example:
>
> <!--{## Ignore} (everything between here and the end HTML comment is commented out) {##/Ignore}-->

33.4.9 Comment Not Put in the Output File: {## COMMENT}

The {##COMMENT} macro allows the template writer to include comments in the template without including them in the final output files. {##COMMENT} provides the functionality of {##ignore}, but the text inside the {##COMMENT} block is not rendered to the output files and is not included in page size calculations. Like {##IGNORE}, {##COMMENT} macros may not be nested.

Syntax

```
{## COMMENT}
 any HTML or other {##}macros
{## /COMMENT}
```

33.4.10 Including Other Templates: {## INCLUDE}

This command allows other templates to be inserted into the current template. It works in a manner similar to the C/C++ `#include` directive.

Syntax

```
{## INCLUDE TEMPLATE=template}
```

Attribute	Description
TEMPLATE	This attribute gives the name of the template to insert.

33.4.11 Setting Options Within the Template: {## OPTION}

This macro sets an option to a given value. All {##OPTION} statements are executed in the order in which they are encountered. Remember when using this template macro that the {##UNIT} tag must be the first template macro in any template.

Options set in the template have template scope. This means that, for example, if a {##LINK} macro references another template, options in the referenced template are not affected by the option settings from the parent template. Similarly, when the files contained in an archive file are converted, Export recursively calls itself to perform the exports of the child documents in the archive. Each child document is converted using a copy of the parent template, and that copy does not inherit the option values from the parent template.

Options set using {##OPTION} in the template are not inherited by the dynamic conversions performed on files within archives. Each child conversion receives a fresh copy of all option values as originally set with DASetOption.

Remember that setting an option in the template overrides any option value set by an application within the scope of the template.

Syntax

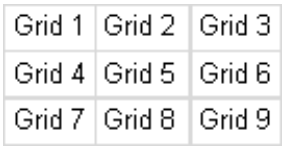
```
{## OPTION OPTION=value}
```

Attribute	Description
OPTION	See the table below for the supported options and their values.

Supported Options and Values

Option	Description
SCCOPT_GRAPHIC_TYPE	This option sets the format of the graphics produced by Dynamic Converter when it converts document embeddings. The supported values are: • **FI_GIF**: GIF graphics • **FI_JPEGFIF**: JPEG graphics • **FI_PNG**: PNG graphics • **FI_NONE**: no graphic conversion The default is FI_JPEGFIF.
SCCOPT_GIF_INTERLACED	This option specifies whether GIF output should be interlaced or non-interlaced. Interlaced GIF graphics are useful when graphics are to be downloaded over slow Internet connections. They allow the browser to begin to render a low-resolution view of the graphic quickly and then increase the quality of the image as it is received. There is no real penalty for using interlaced graphics. The supported values are: • **0** or **FALSE** (that is, non-interlaced) • **1**or **TRUE** (that is, interlaced)
SCCOPT_JPEG_QUALITY	This options sets the lossyness of JPEG compression. This should be a value between 1 and 100 (percent), with 100 being the highest quality but the least compression, and 1 being the lowest quality but the most compression.
SCCOPT_GRAPHIC_SIZEMETHOD	This option determines the method used to size graphics. You can choose among three methods, each of which involves some degree of trade off between the quality of the resulting image and speed of conversion: • SCCGRAPHIC_QUICKSIZING • SCCGRAPHIC_SMOOTHSIZING • SCCGRAPHIC_SMOOTHGRAYSCALESIZING Using the **quick sizing** option results in the fastest conversion of color graphics, though the quality of the converted graphic will be somewhat degraded. The **smooth sizing** option results in a more accurate representation of the original graphic, as it uses anti-aliasing. Anti-aliased images may appear smoother and can be easier to read, but rendering when this option is set will require additional processing time. Please note that the smooth sizing option does not work on images which have a width or height of more than 4,096 pixels. The **grayscale-only** option also uses anti-aliasing, but only for grayscale graphics, and the quick sizing option for any color graphics.

Option	Description
SCCOPT_GRAPHIC_OUTPUTDPI	This option specifies the output graphics device's resolution in dots per inch (dpi), and only applies to images whose size is specified in physical units (in/cm). For example, consider a 1-inch square, 100-dpi graphic that is to be rendered on a 50-dpi device (with this option set to '50'). In this case, the size of the resulting WBMP, TIFF, BMP, JPEG, GIF, or PNG will be 50 x 50 pixels. The valid values are any integer between 0 and 2400 (dpi).
SCCOPT_GRAPHIC_SIZELIMIT	This option sets the maximum size of the exported graphic (in pixels). It may be used to prevent inordinately large graphics from being converted to equally cumbersome output files, thus preventing bandwidth waste. This option takes precedence over all other options and settings that affect the size of a converted graphic.
SCCOPT_GRAPHIC_WIDTHLIMIT	This option allows a hard limit to be set for how wide (in pixels) a converted graphic may be. Any images wider than this limit will be resized to match the limit. It should be noted that regardless whether the SCCOPT_GRAPHIC_HEIGHTLIMIT option is set or not, any resized images will preserve their original aspect ratio. Images smaller than this width are not enlarged when using this option.
SCCOPT_GRAPHIC_HEIGHTLIMIT	This option allows a hard limit to be set for how high (in pixels) a converted graphic may be. Any images higher than this limit will be resized to match the limit. It should be noted that regardless whether the SCCOPT_GRAPHIC_WIDTHLIMIT option is set or not, any resized images will preserve their original aspect ratio. Images smaller than this height are not enlarged when using this option.
SCCOPT_EX_FONTFLAGS	This option is used to turn off specified font-related markup in the output. Naturally, if the requested output flavor or other option settings prevent markup of the specified type from being written, this option cannot be used to turn it back on. However, specifying the size, color and font face of characters may all be suppressed by bitwise OR-ing together the appropriate combination of flags in this option. • **SUPPRESS_SIZE** • **SUPPRESS_COLOR** • **SUPPRESS_SIZECOLOR** • **SUPPRESS_FACE** • **SUPPRESS_SIZEFACE** • **SUPPRESS_COLORFACE** • **SUPPRESS_ALL** • **SUPPRESS_NONE**
SCCOPT_EX_GRIDROWS	This option specifies the number of rows that each template "grid" (applicable only to spreadsheet or database files) should contain. Setting this option to zero ("0") means that no limit is placed on the number of rows in the grid.

Option	Description
SCCOPT_EX_GRIDCOLS	This option specifies the number of columns that each template "grid" (applicable only to spreadsheet or database files) should contain. Setting this option to zero ("0") means that no limit is placed on the number of columns in the grid.
SCCOPT_EX_GRIDADVANCE	This option specifies how the "previous" and "next" relationships will work between grids. • **ACROSS**: The input spreadsheet or database is traversed by rows. • **DOWN**: The input spreadsheet or database is traversed by columns. This option has no effect on up/down or left/right navigation.
SCCOPT_EX_GRIDWRAP	This option specifies how the "previous" and "next" relationships work between grids at the edges of the spreadsheet or database. Consider a spreadsheet that has been broken into 9 grids by HTML Export as follows:  Grid 1 Grid 2 Grid 3 Grid 4 Grid 5 Grid 6 Grid 7 Grid 8 Grid 9 If this option is set to TRUE, then the Grids.Next.Body value after Grid 3 will be Grid 4. Likewise, the Grids.Previous.Body value before Grid 4 will be Grid 3. If this option is set to FALSE, then the Grids.Next.Body after Grid 3 will not exist as far as template navigation is concerned. Likewise, the Grids.Previous.Body before Grid 4 will not exist as far as template navigation is concerned. In other words, this option specifies whether the "previous" and "next" relationships "wrap" at the edges of the spreadsheet or database.

33.4.12 Copying Files: {## COPY}

The {##COPY} macro is used to copy extra, static files into the output directory along with the output from the converted document. For example, if you have added a company logo that was not in the original input document, {##COPY} can be used to make it a part of the converted output document. Other examples include graphics used to mimic buttons for navigation, outside CSS files, or a piece of Java code to be run.

Syntax

```
{## COPY FILE=file}
```

Attribute	Description
FILE	This is the name of the file to be copied. If a relative path name is specified as part of the file, then it must be relative to the directory containing the root template file. For example: {## COPY FILE=uparrow.gif}

The {##COPY} macro may occur anywhere inside a template. If the {##COPY} is inside a {##IF}, then the {##COPY} will only be executed if the condition is TRUE. In {##REPEAT} loops, the {##COPY} will only be performed if the loop is executed one or more times. In addition, if the {##REPEAT} loops more than once, Dynamic Converter detects this and the {##COPY} is executed only once.

As its name suggests, the {##COPY} macro is a straight file copy. Therefore, no conversions are performed as part of the copy. For example, graphics formats are not changed and graphics are not resized. Template authors should also remember to use {##GRAPHIC} when graphics and other files are copied so that space will be created for the external graphic in the text buffer size calculations.

Because the only action Dynamic Converter takes is to copy the requested file, it is up to the template author to make use of the copied file at another point in the template. For example, a graphic file may be copied and then the template can use an <img> tag which references the copied graphic. The following snippet of template code would do this:

```
{## copy FILE=Picture.JPG
{## graphic PATH=Picture.JPG}
<img src="Picture.JPG">
```

> **Note:**
>
> If the file copy fails, Dynamic Converter will continue and no error will be reported.

33.4.13 Deprecated Template Macros

Earlier releases of Dynamic Converter used different macro syntax where template macros were expected to start with {Inso} rather than {##}. In addition some words that had been abbreviated must now be spelled out ("insert" instead of "ins"). The old syntax will continue to be supported for the foreseeable future. However, it has been deprecated.

The old Inso macros and their new equivalents are as follows:

- `{insoins}` is now `{##insert}`
- `{insoif} ... {/insoif}` is now `{##if} ... {##/if}`
- `{insoelseif} ... {/insoelseif}` is now `{##elseif} ... {##/elseif}`
- `{insoelse} ... {/insoelse}` is now `{##else} ... {##/else}`
- `{insoignore} ... {/insoignore}` is now `{##ignore} ... {##/ignore}`

- {insolink} is now {##link}
- {insorep} ... {/insorep} is now {##repeat} ... {##/repeat}

You cannot mix old-style Inso macros with the new {##}macro style in the same template.

No new or future features that Dynamic Converter will include support the old syntax. Thus, for example, the old syntax has not been extended to include support for the new {##UNIT} macros.

33.5 Pragmas

Pragmas provide access to certain document elements that are not logically part of the element tree. The following pragmas are supported:

- Pragma.Charset
- Pragma.CSSFile
- Pragma.EmbeddedCSS
- Pragma.JsFile
- Pragma.SourceFileName

33.5.1 Pragma.Charset

This pragma represents the HTML text string associated with the character set of the characters that Dynamic Converter is generating. In order for Dynamic Converter to correctly code the character set into the HTML it generates, all templates should include a META tag that uses the {##INSERT} macro as follows:

```
<META HTTP-EQUIV="Content-Type" CONTENT="text/html; charset={## INSERT
ELEMENT=pragma.charset}">
```

If the template does not include this line, the user will have to manually select the correct character set in their browser.

33.5.2 Pragma.CSSFile

This pragma is used to insert the name of the Cascading Style Sheet (CSS) file into HTML documents. This name is typically used in conjunction with an HTML <LINK> tag to reference styles contained in the CSS file generated by Dynamic Converter.

When used with the {##INSERT} macro, this pragma will generate the URL of the CSS file that is created. This macro must be used with {##INSERT} inside every template file that inserts contents of the source file and when the selected HTML flavor supports CSS. The CSS file will only be created if the selected HTML flavor supports CSS.

When used with the {##IF} macro, the conditional will be true if the selected HTML flavor supports Cascading Style Sheets or not.

If CSS is required for the output, {##IF element=pragma.embeddedcss} or {##IF element=pragma.cssfile} must be used. However, Dynamic Converter does not differentiate between the two, as the choice of using embedded CSS vs. external CSS is your decision and you may even wish to mix the two in the output.

An example of how to use this pragma that works when exporting either CSS or non-CSS flavors of HTML would be as follows:

```
{## IF ELEMENT=Pragma.CSSFile}
 <LINK REL=STYLESHEET
 HREF="{## INSERT
 ELEMENT=Pragma.CSSFile}">
 </LINK>
{## /IF}
```

33.5.3 Pragma.EmbeddedCSS

This pragma is used to insert CSS style definitions in a single block in the <HEAD> of the document.

When used with the {##INSERT} macro, this pragma will insert the block of CSS style definitions needed for use later in the file. This macro must be used inside every output HTML file where {##INSERT} is used to insert document content.

When used with the {##IF} macro, the conditional will be true if the selected HTML flavor supports CSS.

If CSS is required for the output, {##IF element=pragma.embeddedcss} or {##IF element=pragma.cssfile} must be used. However, Dynamic Converter does not differentiate between the two, as the choice of using embedded CSS vs. external CSS is your decision and you may even wish to mix the two in the output.

If a style is used anywhere in the input document, that style will show up in the embedded CSS generated for all the output HTML files generated for the input file. Consider a template that splits its output into multiple HTML files. In this example, the input file contains the "MyStyle" style. It does not matter if during the conversion only one output HTML file actually references the "MyStyle" style. The "MyStyle" style definition will still show up in the embedded CSS for all the output files, including those files that never reference this style.

33.5.4 Pragma.JsFile

This pragma is used to insert the name of the JavaScript file into HTML documents. This name is typically used in conjunction with an HTML <SCRIPT> tag to reference JavaScript contained in the `.js` file generated by HTML Export.

When used with the {##INSERT} macro, this pragma will generate the URL of the JavaScript file that is created. This macro must be used with {##INSERT} inside every template file that inserts contents of the source file when:

1. The selected HTML flavor supports JavaScript.
2. The javaScriptTabs option has been set to true.

The JavaScript file will only be created if the selected HTML flavor supports JavaScript.

When used with the {##IF} macro, the conditional will depend upon whether the selected HTML flavor supports JavaScript or not.

33.5.5 Pragma.SourceFileName

This pragma represents the name of the source document being converted.

> **Note:**
>
> The Pragma.SourceFileName pragma does ***not*** include the path name.

33.6 Setting Script Template Formatting Options

You can control formatting options for script templates by editing the Script Template Conversion Configuration Settings on the Dynamic Converter Configuration page.

The settings that you can change include:

- Changing the Format Used for Converted Graphics
- Generating Bullets and Numbers for Lists

33.6.1 Changing the Format Used for Converted Graphics

If you want to change the format to be used for converted graphics, edit the following option:

```
# SCCOPT_GRAPHIC_TYPE
#
# Determines what graphic format will be used for exported graphics.
# Setting this to "none" disables graphic output.
#
graphictype gif
#graphictype jpeg
#graphictype png
#graphictype none
```

Lines that begin with "#" have been commented out. So the above example shows the default setting, with the `.gif` format selected. To use the `.jpeg` format, instead, you would simply comment the first line and uncomment the second line, thus:

```
#graphictype gif
graphictype jpeg
#graphictype png
#graphictype none
```

33.6.2 Generating Bullets and Numbers for Lists

If you want to generate bullets and numbers for lists instead of HTML list tags, you would edit the following option:

SCCOPT_GENBULLETSANDNUMS

```
#
# Generate Bullets and Numbers. Bullets and numbers will be generated for
# lists instead of using HTML list tags (<ol>, <ul>, <li>, etc.) when
# rendering lists in a document.
#
genbulletsandnums no
#genbulletsandnums yes
```

Again, comment one line and uncomment another, thus:

```
#genbulletsandnums no
genbulletsandnums yes
```

33.7 Breaking Documents by Structure

One of the most powerful features of the template architecture is the ability to break long word processor documents up into logical pieces and create powerful navigation aids to access them.

To understand how this is done, you must first understand the document tree as it relates to word processing documents. The somewhat complex graphic below attempts to show how the elements in the tree relate to a real-world document (see figure below).

The following are some examples of elements and the data they would produce if run against the document shown in the preceding image. Note the omission of the default nodes *body* and *contents* in the second two examples:

```
body.contents.headings.2.body.title
```

would produce "Present Day."

```
body.contents.headings.2.body.contents.headings.1.body.title
```

would produce "Commercial."

```
body.contents.preface
```

would produce "The History of Flight" and the text below it, up to but not including "Introduction."

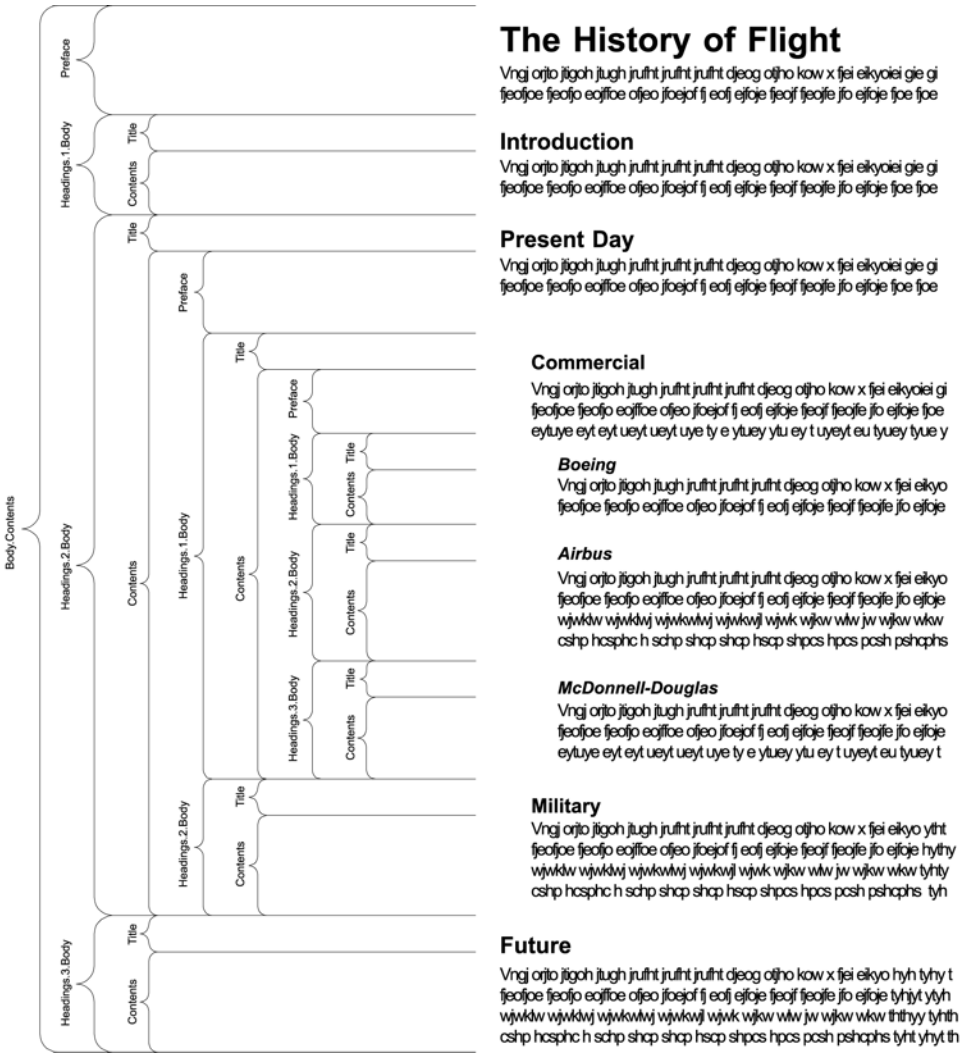
```
headings.2.headings.1.headings.3.title
```

would produce "McDonnell-Douglas."

```
headings.2.headings.1.headings.3.contents
```

would produce the text below "McDonnell-Douglas" but above "Military."

Figure 33-2 Breaking Up Documents by Structure



Breaking documents requires that Dynamic Converter understands the logical divisions in the structure of a document. Currently the only formats that can give Dynamic Converter this information in an unambiguous manner are Microsoft Word 95 and higher and WordPerfect 6.0 and higher. In these formats, the breaking information is available if the author placed table-of-contents information in the document. Refer to the appropriate software manual for information on the necessary procedure for including this information. That is not to say that the document must have a table of contents, only that the information to build one must be present.

It should be noted that some word processing formats, including Microsoft Word 2002 (XP), allow users to specify TOC entries in multiple ways. Dynamic Converter only supports two of these methods:

TOC specified through…	Supported in Dynamic Converter?
Applied heading styles	Yes
Custom styles with outline levels	Yes

TOC specified through…	Supported in Dynamic Converter?
Outline level applied as a paragraph attribute	No
TOC entries	No

Additionally, if a heading style is applied to text inside a table in the original document, Dynamic Converter will not break on that heading. This is because Dynamic Converter will not break within tables.

Indexes and Structure-Based Breaking

All repeatable nodes have an associated index variable that has a current value at any given time in the conversion process. For elements that contain repeatable nodes as part of their path, the instance of the repeatable element must be specified by using a number or one of several index variable keywords. For more information on the possible values for the index variables, see Index Variable Keywords.

33.8 Breaking Documents by Content Size

In addition to breaking documents by structure (see Setting Script Template Formatting Options), Dynamic Converter also supports breaking documents based on the amount of content to be placed in each output file or "page." Documents can even be broken based on both their structure *and* content size.

To break documents by content size, two things must be done. First, the `SCCOPT_EX_PAGESIZEpageSize` option must be set (see Setting Options Within the Template: {## OPTION}). The second thing that must be done is that the template used must be equipped with the {##UNIT} construct (see Units: {## UNIT}, {## HEADER}, and {## FOOTER}).

The basic idea behind the unit template construct is to tell Dynamic Converter what things should be repeated on every "page" and what pieces should only be shown once. In other words, the unit template construct provides a mechanism for grouping template text and document elements. Unit boundaries are used when determining where to break the document when spanning pages.

Here are some examples of the kinds of things the template author might want to appear on every page:

- The <META> tag inserting the output document character set.
- A company copyright message.
- Navigational elements to link the previous/next pages together.

Typical examples of things that would not go on every page would be:

- The actual content of the document.
- Structural navigational elements like the links for a table of contents.

A unit consists of a header, a footer (both of which are optional), and a body. Items that are to be repeated at the beginning or end of every unit should be placed in the header or footer respectively.

A unit is delimited by the {##UNIT} template macro. Similarly, the {##HEADER} and {##FOOTER} template macros delimit the header and footer respectively. The body is everything that is left between the header and the footer. The {##UNIT} macro must be

the first macro in the template. The body frequently contains nested units. The body may be empty.

To ensure that the header is the first item in the template and the footer is the last item, text between the {##UNIT} tag and the {##HEADER} tag will be ignored, as will text between the {##/FOOTER} tag and the {##/UNIT} tag, including whitespace. The header and footer of a unit will be output in every page containing that unit, enclosing that portion of the unit's body that is able to fit in a particular page. The entire template is a unit that may contain additional units.

33.8.1 A Sample Size Breaking Template

By way of example, let's take another look at the very simple template from About Script Templates. To make things more interesting, let's insert the character set into the template with a <meta> tag. Let's also insert some better navigation to improve movement between the pages. The modified version of the template is as follows:

```
{## unit}{## header}
<html><head>
<meta HTTP-EQUIV="Content-Type" CONTENT="text/html;
charset={## insert element=pragma.charset}" /></head>
<body>
{## anchor aref="prev" format="<p><a href=\"%url\">Prev</a></p>"}
{## /header}
<p>Here is the document you requested.
{## insert element=property.title} by
{## insert element=property.author}</p>

<p>Below is the document itself</p>
{## insert element=body}
{## footer}
{## anchor aref="next" format="<p><a href=\"%url\">Next</a></p>"}
</body>
</html>
{## /footer}{## /unit}
```

A very small value (about 20 characters) is used for the page size option. The resulting HTML might look like this (HTML that is the result of a macro is in **bold**):

file1.htm

```
<html><head>
<meta HTTP-EQUIV="Content-Type" CONTENT="text/html; charset=us-ASCII"/></head>
<body>
<p>Here is the document you requested.</p>
<p>A Poem by Phil Boutros</p>
<p><a href="file2.htm">Next</a></p>
</body>
</html>
```

file2.htm

```
<html><head>
<meta HTTP-EQUIV="Content-Type" CONTENT="text/html; charset=us-ASCII" /></head>
<body>
<p><a href="file1.htm">Next</a></p>
<p>Below is the document itself</p>
<p>Roses are red</p>
<p>Violets are blue</p>
```

```
<p><a href="file3.htm">Prev</a></p>
</body>
</html>
```

file3.htm

```
<html><head>
<meta HTTP-EQUIV="Content-Type" CONTENT="text/html; charset=us-ASCII" /></head>
<body>
<p><a href="file2.htm">Prev</a></p>
<p>I'm a programmer</p>
<p>and so are you</p>
</body>
</html>
```

There are several things to note here:

- The page size option value does not apply to the text from the template, only the text inserted from the source document. Each page contains roughly 20 characters of visible input document text.
- The {##INSERT} of the character set is part of the {##HEADER} and therefore is inserted into all the output pages.
- Text from the body of the unit is inserted sequentially. Thus "as is" template text such as the line " Below is the document itself " is only inserted once.
- The {##ANCHOR} tags only insert links to the previous/next page if there actually is a previous/next page. Thus the first page does not have a link to the non-existent previous page.

33.8.2 Templates Without {## UNIT} Macros

The {##UNIT} macro is only required in templates that are designed to break pages based on size using the `SCCOPT_EX_PAGESIZEpageSize` option. An example of a template that would not perform any size-based breaking is one that defines an HTML <FRAME>, but does not include any document content. Another example where size-based breaking might not be work is a table of contents page, even though a table of contents page does contain document content.

A template that does not conform to the {##UNIT} format is a not a size-based breaking template. Support for this type of template will continue for the indefinite future. The template will be considered to not be a size-based breaking template if the first macro tag encountered is something other than {##UNIT}. This means that there cannot be any {##UNIT}, {##HEADER} or {##FOOTER} macros later in the template. The value of the `SCCOPT_EX_PAGESIZEpageSize` option will be ignored for this type of template.

33.8.3 Indexes and Size-Based Breaking

As mentioned earlier, all repeatable nodes have an associated index variable. For information about using index variable keywords such as "Next" and "Last," see Index Variable Keywords.

33.9 Using Grids to Navigate Spreadsheet and Database Files

In order to support spreadsheets (and database files, though they are not as common), a template-based navigation concept known as a "grid" is available. Grids offer a way to consistently navigate a spreadsheet or database in an intuitive fashion.

Grids can be used to present the output of large spreadsheets in smaller pieces, so that less scrolling is necessary. It can also be used to help prevent the HTML versions of large spreadsheets from overwhelming browsers, potentially causing them to lock up. Grids can also be used to halt processing of large spreadsheets before they waste too much CPU time.

To use grids, you should use the new grid template element (see Element Definitions). Grids may only be used in templates that have been enabled with the {##UNIT} template macro. It is also important to set the grid-related options (see Setting Options Within the Template: {## OPTION}).

The grid support has some important limitations:

1. The output file format and flavor are expected to supports tables, although this is not required.
2. Grids are only used when converting spreadsheets and database input files. Grids are not available for word processing files at this time.
3. Due to size constraints, grid support works best if the contents of the cells in the input file do not make use of a lot of formatting (bold, special fonts, text color, etc.).

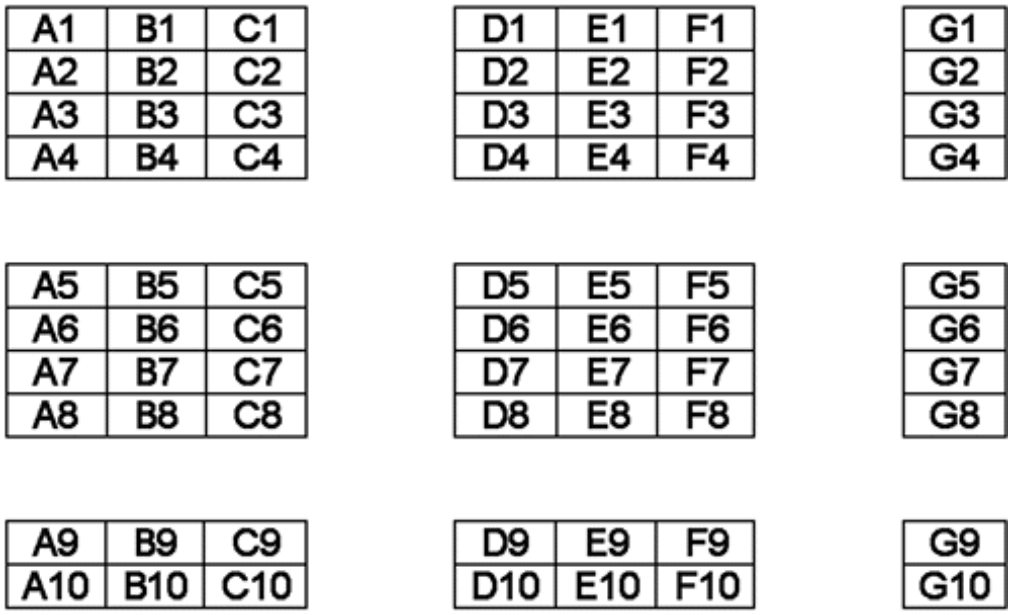
To further explain the grid system, consider a multi-sheet spreadsheet workbook as an example. Each sheet in the spreadsheet workbook is broken into a collection of grids. Each grid has a fixed maximum size and is a rectangular portion of the spreadsheet. The size of the grid is specified as a number of spreadsheet cells. For example, consider the 7 x 10 spreadsheet in Figure 33-3.

Figure 33-3 Example 7 X 10 Spreadsheet

A1	B1	C1	D1	E1	F1	G1
A2	B2	C2	D2	E2	F2	G2
A3	B3	C3	D3	E3	F3	G3
A4	B4	C4	D4	E4	F4	G4
A5	B5	C5	D5	E5	F5	G5
A6	B6	C6	D6	E6	F6	G6
A7	B7	C7	D7	E7	F7	G7
A8	B8	C8	D8	E8	F8	G8
A9	B9	C9	D9	E9	F9	G9
A10	B10	C10	D10	E10	F10	G10

If you wanted to break it up into 3 x 4 grids, nine grids would be produced as shown in Figure 33-4.

Figure 33-4 Example 7 x 10 Spreadsheet Split Up in 3 X 4 Grids



Normally, all grids have the same number of cells. The exception is that grids at the right or bottom edge of the spreadsheet may be smaller than the normal size. Grids will never be larger than the requested size. For this reason, grids can easily be navigated by using "up," "down," "left," or "right." One thing that grids cannot do is address individual cells in a spreadsheet (except, of course, in the case of a grid whose size is 1 x 1).

Dynamic Converter does not force deck/page breaks between each grid. Therefore, if the template writer wants to limit each deck/page to only one grid, they should force the break in the template.

Grid Support When Tables Are Not Available

Not all output flavors supported by Dynamic Converter support the creation of tables. If the output flavor does not support tables, Dynamic Converter will still support grids. However, Dynamic Converter's normal non-table output will be what is presented in grid form. For example, if "[A1]" represents the contents of cell A1, then we would export the following for a grid of size (2 x 2):

If `grids.1.body` is:

```
[A1]
[A2]
[B1]
[B2]
```

then `grids.right.body` is:

```
[C1]
[C2]
[D1]
[D2]
```

and `grids.down.body` is:

```
[A3]
[A4]
[B3]
[B4]
```

34
Working with Converted Content

This chapter provides information on working with content items that have been converted and checked in to the Oracle WebCenter Content Server.
This chapter covers the following topics:

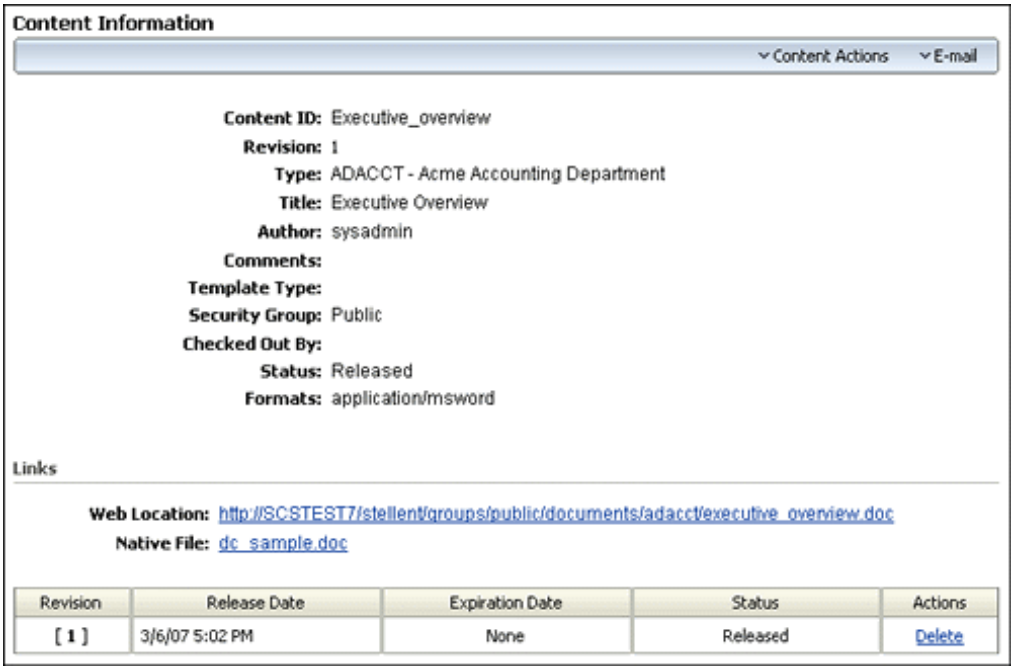
- Viewing Content Information
- Viewing a Converted File
- Previewing a Document Before Check-In

34.1 Viewing Content Information

Every content item checked into the Content Server has its own content information page, which can be used to view and verify the metadata information about the content item, such as the content ID, title, author, and other metadata (see Figure 34-1). You will frequently visit the content information page of your source documents in order to specify your template selection rule criteria.

The Info icon on the search results page is used to access the content information page of a content item, where you can view the metadata for the content item. Use this page to view and verify information about a specific content item. For example, you can identify the release date of a file or the user login of the author.

Figure 34-1 Content Information Page

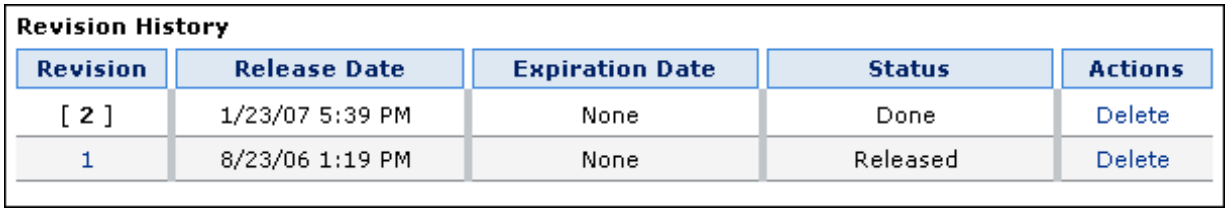


This page shows a lot of information about the content item, including:

- Values for all the metadata fields that were completed when the file was checked into the Content Server
- The author's name (user login)
- The file status indicating where the file is in its life cycle
- The file format, which is the native application that the file was created with. The file format is expressed as the MIME content type.
- The current web location, which is an active link that points to the web-viewable rendition (for example, PDF) of the checked-in content item, if such a rendition was generated. This URL uniquely refers to the web-viewable rendition of the content item's latest revision.
- A native file link, which you can use to get a copy of the content item in its native format (that is, the one it was originally created in). If you click the link, you can open the file in its native application (if you have it installed on your computer) or you can save it to your local hard drive. You can also right-click the link and save the file locally. This enables you to make a copy of the file for reuse. You can then check it back into the Content Server as a new revision.
- The complete revision history. See an example in Figure 34-2.

> **Note:**
>
> The content information can be displayed for any revision of the content item by clicking the revision link that is displayed in the Revision column of the Revision History section. The currently displayed content item is enclosed in square brackets: [].

Figure 34-2 Revision History of Content Item


Revision History

Revision	Release Date	Expiration Date	Status	Actions
[2]	1/23/07 5:39 PM	None	Done	Delete
1	8/23/06 1:19 PM	None	Released	Delete

The content information page has other functions in addition to viewing a file's metadata, status, and revision history. The available options depend on your assigned privileges and the Content Server configuration, and may include any of the following:

Action	Definition
Check Out	Enables you to check out a file for edit and later check it in with the same content ID and the revision number incremented by one (if you are a contributor).

Action	Definition
Undo Check Out	Cancels the check-out of the content item. Your name will no longer appear next to "Checked out by: on the content information page. You can only undo a check-out of a content item that you checked out if you have the "admin" role or have administrator permissions for the security group that the content item belongs to.
Check In	Checks in a new revision of a content item currently checked out.
Update	Enables you to change the metadata fields for a content item already checked into the Content Server. For example, you can use Update to correct a misspelled word in the title field or select the correct content type if you initially entered it incorrectly.
Check In Similar	Enables you to check in another content item with the same metadata of the content item you have just checked in.
Send link by email	Opens your email program with a new message that contains a link to the URL (web address) of the web-viewable file.
Subscribe	Enables you to tag a content item so that you are automatically notified by email about any changes to it (that is, if a new revision is checked in). If the software does not know your email address, you are prompted to enter it.
Unsubscribe	Enables you to cancel your subscription to the content item (that is, no longer be notified of new revisions).
Create Shortcut	Enables you to create a shortcut to the content item in the Content Server and store the shortcut in a folder under Browse Content.
Delete Revision	Enables you to remove a revision of a file from the system. To delete a revision, you must have delete permission for the security group the file belongs to.
Revision Number	Displays the content information for the specified revision.

To access the content information page of a content item, complete the following steps:

1. Search for the content item.

   The search results page is displayed.

2. Click the Info icon (Figure 34-3) that corresponds to the file for which you want to see the content information.

Figure 34-3 Info Icon

The content information page is displayed.

> **Note:**
>
> For more information on searching for content, see *Using Oracle WebCenter Content*.

34.2 Viewing a Converted File

Dynamic Converter provides a solution to the problem of requiring a client workstation to have native applications installed (such as Microsoft Word, Excel, or other applications) in order to open source documents created with those applications. It does this by creating a web-viewable version of the source document on demand and on the fly.

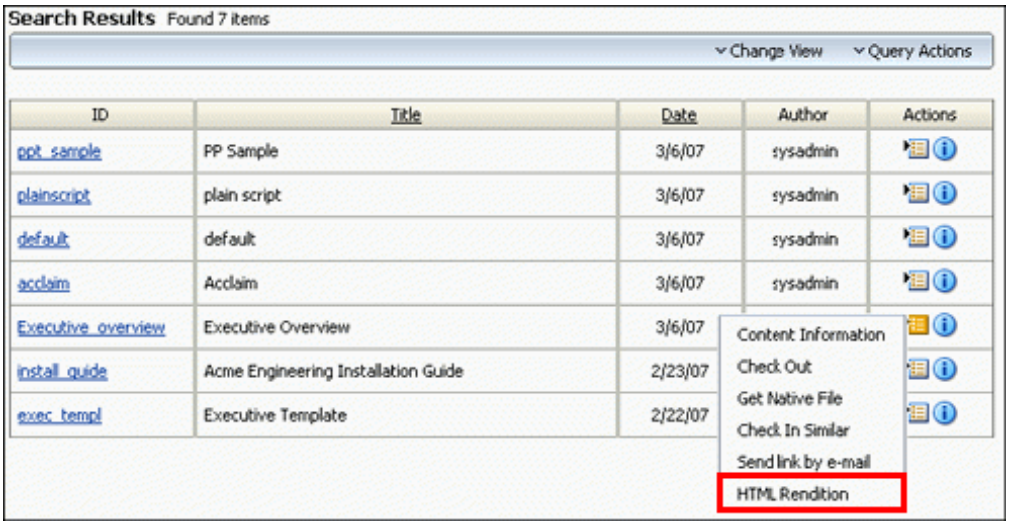
The web-viewable version of the source document can be seen by clicking an HTML link on these Content Server pages:

- Search Results Page
- Content Information Page

34.2.1 Search Results Page

You can use the extensive search Element to find content items. You can search by metadata and/or perform a full-text search (depending on the Content Server setup). The results of a search are shown on a search results page. If a content item in the list is of a file type that is supported and enabled for HTML conversion, then an **HTML Rendition** link is included in the actions popup menu. You can use this link to view an HTML rendition of the content item (see Figure 34-4).

Figure 34-4 Html Rendition Link on Search Results Page



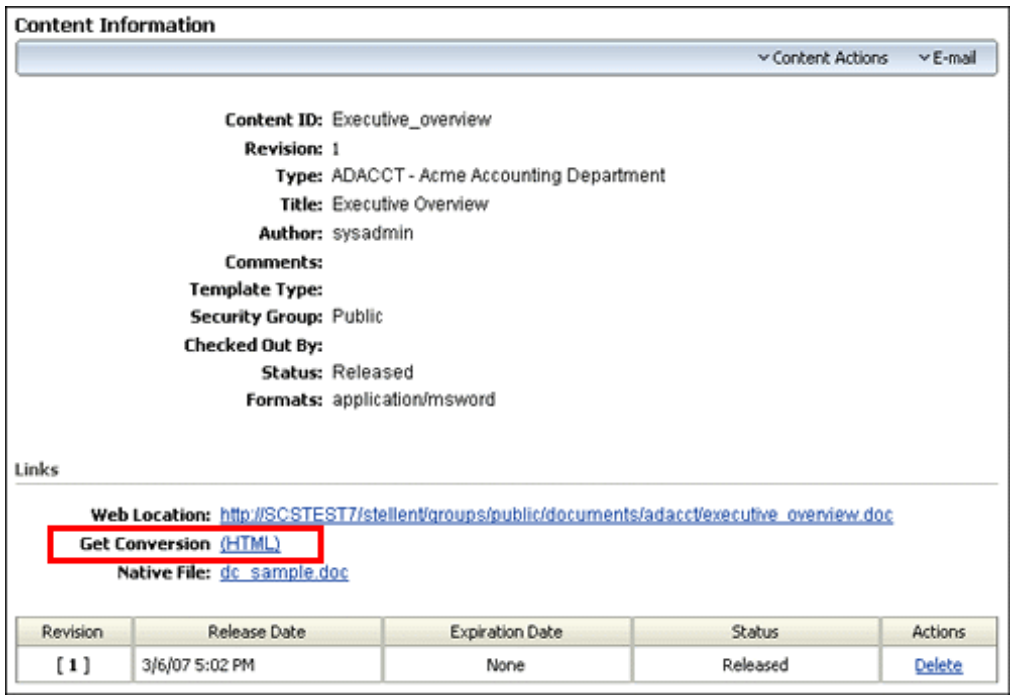
When you click the **HTML Rendition** link, the file is converted and displayed using the rules and templates specified on the Template Selection Rules page.

34.2.2 Content Information Page

Every content item checked into Content Server has its own content information page, which shows the metadata information of the content item, such as the content ID, title, author, and other metadata.

If the content item is of a file type that is supported and enabled for HTML conversion by Dynamic Converter, then the content information page will display an **(HTML)** link beside the text "Get Conversion." You can use this link to view an HTML rendition of the content item (see Figure 34-5).

Figure 34-5 Html Link on Content Information Page

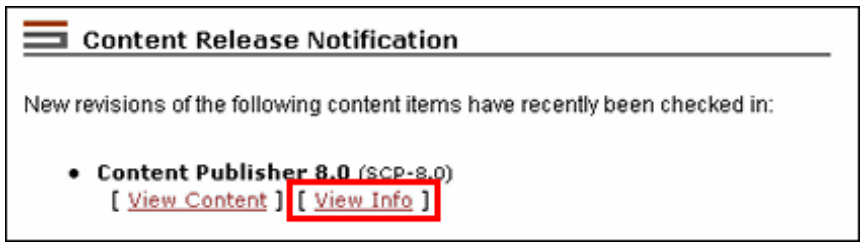


When you click the **(HTML)** link, the file is converted and displayed using the rules and templates specified on the Template Selection Rules page.

Subscription and Workflow Notifications

You can also open the content information page using the **View Info** link in the e-mail messages that you receive when you subscribe to a content item stored in the Content Server (see Figure 34-6).

Figure 34-6 View Info Link in Subscription Email Notification Message



This same link is available in workflow notification messages, which eliminates the need for content reviewers to have the native application used to create the source file.

34.3 Previewing a Document Before Check-In

Content contributors can preview the HTML rendition of a document before checking it into the Content Server. This enables them to see if there are problems with the document or the template associated with the document, and notify the site webmaster or developer. Problems can then be resolved before more users or customers view the converted content. Both the content authors and the site developers gain from the ability to preview documents this way.

The dynamic contributor preview is displayed as an **(HTML)** button on Content Server's content check-in page (see Figure 34-7).

Figure 34-7 Html Preview Button on Content Check-In Screen

Once a document has been selected and all metadata assigned to the document, click the preview button to see how the document will appear as a web page. The resulting screen displays a **Complete Check In** link in the left frame and the converted document in the right frame (see Figure 34-8).

Figure 34-8 Dynamic Conversion Preview

If you are satisfied with the HTML rendition of the document, you can click **Complete Check In** to check the document into the Content Server (at which time you are brought to the check-in confirmation screen). Click the **Back** button in your web browser to cancel the process and return to the content check-in screen.

If you check in a document using metadata that has no template associated with it, a blank Classic HTML Conversion template is assigned. This template contains no special formatting instructions, other than to convert your document into a web page.

> **Tip:**
>
> As a site administrator, you can also preview how a content item will appear with a particular template using the **Change Preview** button in the Template Editor.

35
Implementation Considerations

This chapter provides information about some of the more pragmatic concerns when dealing with Dynamic Converter.
This chapter covers the following topics.

35.1 Metadata Fields With Multi-Byte Characters

The new Dynamic Converter HTML Template Editor does not support working with multi-byte content IDs for the templates or the content items being converted. It is recommended that you do not use multi-byte characters in your content IDs, security groups, content types, and account names, even if Dynamic Converter is used in a multi-byte environment (Japanese, Korean, or other non-Roman alphabets). This content metadata information is included in the URL of a content item, and limitations in current web technology may prevent web servers and web browsers from handling multi-byte character URLs correctly. (Dynamic Converter, for example, will fail to locate content items if the links are broken.)

If you want to use multi-byte characters in content IDs, security groups, content types, or accounts, you need to make sure that the entire Oracle WebCenter Content Server environment (servers and clients) runs on operating systems that support multi-byte languages (for example, Japanese or Korean versions of Microsoft Windows).

35.2 Conversion of PDF Files in UNIX

Conversion of PDF files under UNIX may be slow and may time out after three minutes (the default timeout value for the conversion process).

To increase the conversion timeout, complete the following tasks:

1. Open the Dynamic Converter Admin page.
2. Click **Configuration Settings**.
3. On the Dynamic Converter Configuration page, enter a new value in the **Time Out** field (increasing it from 3 minutes, which is the default).
4. Click **Update** to enable your changes.

The changed setting takes effect immediately, so you do not need to restart the Content Server.

35.3 Embedded Graphics on UNIX

Some source documents contain embedded OLE objects. Embedded OLE objects are usually accompanied by a graphic "snapshot" in the form of a Windows metafile. On both Windows and UNIX, Dynamic Converter can use the metafile snapshot to convert the OLE object. When the metafile is not available, Dynamic Converter reverts to OLE technologies for the conversion. In that event, the conversion will still succeed on Windows, but it will fail on UNIX.

35.4 Use of Vector Versus Raster Graphics Formats

If you are converting vector graphics, Dynamic Converter requires access to a running X-Server. This is because Dynamic Converter depends on the X-Server system to draw the pixels.

Access to a running X-server is required only if the OIT internal rendering engine is not used because of either of the following reasons:

- The **Use X-Windows for Rasterization** option is checked on the Dynamic Converter configuration page.
- The OIT internal rendering engine isn't supported on the platform being used.

  The internal OIT rendering engine is supported in Linux, Solaris Sparc, AIX, and HP-UX RISC.

Vector graphics formats describe lines and fills. Common formats are WMF, EMF, CorelDRAW, Adobe Illustrator, Excel charts, Word autoshapes, and PowerPoint presentations. Raster graphics, on the other hand, contain pixel information of an image. Common file formats are BMP, JPEG, and GIF.

One way to tell the difference between a vector and a raster graphic is to try to stretch the image. Because vector graphics describe lines, they will re-compute the placement of the lines and the image should still look nice. Raster graphics, however, will become pixelated when you resize.

For instructions on how to set up rendering of graphics and fonts in UNIX, see Setting Up Fonts on a UNIX System in *Installing and Configuring Oracle WebCenter Content*.

35.5 Converting Vector Graphics and Spreadsheet Text in UNIX

Dynamic Converter requires access to a running X-Server in UNIX in order to convert vector graphics and to properly measure text that spans multiple columns in spreadsheets.

Access to a running X-server is required only if the OIT internal rendering engine is not used because of either of the following reasons:

- The **Use X-Windows for Rasterization** option is checked on the Dynamic Converter configuration page.
- The OIT internal rendering engine isn't supported on the platform being used.

  The internal OIT rendering engine is supported in Linux, Solaris Sparc, AIX, and HP-UX RISC.

35.6 URL Rewriting

Dynamic Converter wraps the `dcUrl('url', reserved_type)` Idoc Script extension function around all links and image source links (`src`). The default implementation of this script function is to do a simply pass-through, but external integration technologies (such as CIS) can modify this behavior by defining a filter plug-in for "dcUrlFilter."

Dynamic Converter evaluates the link URL, applies the "dcUrlFilter" filter if it exists, and then returns the URL value. If the dcUrlFilter filter is not defined, then the original URL is unchanged. Links to internal bookmarks always remain unchanged.

Reserved Types

The `reserved_type` function argument is a number 1001, 1002, and so forth, which indicates where in the Dynamic Converter core engine the URL is being written. This value can be used to distinguish the type of URL. For example, gallery graphic, inter-document link. The reserved type values and their meanings are as follows:

Value	Description
1001	Link (different split)
1002	Previous element (different split)
1003	Previous page (TOC frame)
1004	Previous page
1005	Next page (TOC frame)
1006	Next page
1007	Next element (different split)
1008	Previous page (TOC frame)
1009	Previous page
1010	Next page (TOC frame)
1011	Next page
1018	Image link
1019	Image link
1020	Image link

Value	Description
1021	Image link
1022	Background graphic (not from source)
1023	Background graphic (from source)

35.7 Relative URLs in Templates and Layout Files

Consider the following image tag: `<IMG SRC="image.gif">`. In most implementations of Dynamic Converter, it is likely that the output files will end up in a different location than the template files. If the developer uses the template above in this scenario, the output files produced will have a reference to `image.gif`, which the browser will assume has the same path as the output files. The problem is that `image.gif` is likely to be back in the directory where the template file is located. This is a problem for anything referenced in the template using a relative URL. There are several possible solutions to this problem.

Solution 1: Ensure That the References Are Good

If the developer knows exactly which files all of the templates reference, the correct files (such as `image.gif`) can be moved to or located in the output directory or directories. This solution requires the developer to have exact knowledge of the contents of the templates, and may propagate the same set of files into many output locations.

Solution 2: Use Absolute URLs

The developer can design templates to contain absolute URLs to any referenced files. The template in the example would then look something like this.

```
<HTML>
<BODY>
<P><IMG SRC="http://www.company.com/templates/image.gif"></P>
{## INSERT ELEMENT=Sections.1.Body}
</BODY>
</HTML>
```

If `<$HTTPWEBROOT$>` is used instead, you eliminate the problem of output files tied to a specific domain.

Solution 3: Make Path Statements in a Separate File

The developer can create a separate Idoc Script file that states the path, for example:

```
<@dynamichtml Image_Dir@><$HttpWebRoot$>groups/public/documents/graphic/<@end@>
```

The developer can then load the Idoc resource and reference the path statement from the included Idoc Script file as follows:

```
<img src="<$include Image_Dir$>logo.gif">
```

All long as the graphics (or related files) are checked in with the security group and document type to match the stated path (in this example, a security group "Public" and a document type "Graphic"), then the paths will resolve, and the page will display properly.

35.8 Browser Caching

In the process of building and debugging templates, you are likely to run the same source file through Dynamic Converter repeatedly with slightly different templates. Depending on how you are naming the output files, this may have a tendency to produce the same set of file names repeatedly. In this scenario, especially if the output is being read directly from a file system and not through a web server, browsers will have the tendency to show the old cached results and not the new ones.

If it looks like bad output, click **Refresh** on every frame before deciding that it is a problem with the template or the software.

> **Tip:**
>
> You may find it simpler to empty and turn off caching in your browser while creating and testing your templates.

35.9 Image Sizing Rules

There are a large number of factors that affect the size of the final exported image. The precedence of rules for how those factors work is as follows:

1. Any images that the template specifies with the `{##graphic}` macro are subtracted from the space available for graphics on that particular deck. In general, you should be wary of templates that require images on every deck as they will eat into the overall amount of room available for document graphics.
2. The `SCCOPT_EX_GRAPHICBUFFERSIZE` option, which is only used to reduce image size if necessary. It preserves the image aspect ratio.
3. The `SCCOPT_GRAPHIC_SIZELIMIT` option, which is only used to reduce image size if necessary. It preserves the image aspect ratio.
4. The `SCCOPT_GRAPHIC_WIDTHLIMIT` and `SCCOPT_GRAPHIC_HEIGHTLIMIT` options. These are only used to reduce image size if necessary. They preserve the image aspect ratio, even if both are specified.
5. `'Width='` and `'height='` parameters in the `{##INSERT}` statement of the template. This reduces or enlarges the image to match the specified dimension(s). The image aspect ratio is changed if both are specified. The aspect ratio does not change if only one or none of these parameters is specified.
6. Original image dimensions based on the information in the source file and the DPI setting, if applicable.

35.10 CSS Considerations

The styles discussed in this section relate only to script templates (see Managing Script Templates).

One of the most powerful features of cascading style sheets (CSS) is the ability to override the styles suggested in various ways. Dynamic Converter has designed its CSS support to permit users to override the style sheets that it produces. This, in turn, enables the user to

help blend documents from many authors into a collection that has a more unified look. In order to make this override work, one first needs to understand style names.

In addition, it should be remembered that the output from Dynamic Converter might be placed into many HTML files. Special attention must be paid to ensure that `<LINK REL=STYLESHEET HREF="{## INSERT ELEMENT=Pragma.cssFile}">` statements are placed in the appropriate locations.

35.11 Style Names Used by Dynamic Converter

Style names are taken from the original style names in the source document. There is an inherent limitation in the style names the CSS standard permits. The standard only permits the characters a-z, A-Z, 0-9, and dash (-) . Source document style names do not necessarily have this restriction. In fact, they may even contain Unicode characters at times. For this reason, the original style names may need to be modified to conform to this standard. To avoid illegal style names, Dynamic Converter performs the following substitutions on all source style names:

- If the character is "-," then it is replaced with "--."
- If the character is not one of the remaining characters (a-z, A-Z, or 0-9), then it is replaced by "-xxxx" where "xxxx" is the hexadecimal Unicode value of the character.
- If neither of the preceding situations is applicable, the character appears in the style name normally.

An example of one of the most common examples of this substitution is that spaces in style names are replaced with "-0020." For a more complete example of this character substitution in style names, consider the source style name "My Special H1-Style!" (with a space and an exclamation mark in its name). This would be transformed to "My-0020Special-0020H1--Style-0021."

While admittedly this system lacks a certain aesthetic, it avoids the problem of how the document looks when the browser gets duplicate or invalid style names. Developers should also appreciate the simplicity of the code needed to parse or create these style names.

In addition, Dynamic Converter creates special list versions of styles. These have the same name as the style they are based on with "--List" appended to the end. These styles differ from their original counterparts in that they contain no block-level CSS.

35.12 Overriding Dynamic Converter Styles

Once style names are understood, it is easy to override the CSS file produced by Dynamic Converter. Follow the CSS file link in the template with another link to the CSS override file. For more information on the link to Dynamic Converter's CSS file, see Pragma.CSSFile and {## LINK}. This override file should then contain styles with the same names as the ones used by Dynamic Converter's CSS file.

Remember that many file formats allow styles to be based on other previously defined styles. Dynamic Converter supports this by nesting styles. In this way each nested style inherits and may override items defined in the styles that surround it.

35.13 Pragma.CSSFile and {## LINK}

One {##INSERT Element=Pragma.CSSFile} statement should appear at the top of each HTML file produced when a CSS flavor of HTML is used. It should therefore be remembered that the ##LINK statement may be used to trigger the creation of additional HTML files. As a result, each ##Linked template will typically contain a <Link> tag to the CSS file generated.

Using a ##LINK statement, it is possible, though, to link to a template that does not have any {##}statements that would need to reference the CSS file. In that case, the <Link> to the CSS file may safely be omitted. Consider, for example, a template that has only two ##statements, both of which are ##links (perhaps to put the results into two separate frames). This template file would not need a <Link> to the CSS file.

Regardless of how many HTML files are produced by Dynamic Converter, only one CSS file is generated. It is also worth repeating here that the <Link> to the CSS file must occur in the <HEAD> section of the document and each resulting HTML file may have only one <HEAD> section.

35.14 Well-Formed HTML

The output of Dynamic Converter has been tested to ensure that it is well-formed. This is meaningless, however, unless the template used by Dynamic Converter is also well-formed. To assist with creating well-formed templates, here is a list of common problems that may cause documents to not be well formed:

- All tags must be properly nested.
- All tags that are opened must also be closed. This includes tags that are not normally thought of as needing closing tags, including <META>, <LINK>, <FRAME>, <HR>, and
.
- Everything after an is-equal-to sign (=) must be in double quotes. Hence, <FONT COLOR="0000FF"> is OK, but <FONT COLOR=0000FF> is not.
- In order for   to appear in a document, a <!DOCTYPE> statement must be in the HTML code. Because Dynamic Converter cannot know if the template included the <!DOCTYPE> statement when the SCCHTML_FLAG_STRICT_DTD flag is set,   is always used instead of .
- Characters in the range 0x80 - 0xFF are to be written in the form &#xxx;.
- The only three characters < 0x20 allowed in any document are: \t, \n, and \r.
- All attributes of a tag must be followed by "=value". Thus, the NoWrap in <Table NoWrap> is not well formed. Dynamic Converter uses <Table NoWrap=NoWrap> instead.

35.15 Positional Frames Support

Dynamic Converter 7.7 and higher uses DHTML to position objects. However, only two types of object positioning are supported: *paragraph anchored objects* and *page anchored objects*. Here are some important notes about this initial support for positional frames:

- Dynamic Converter generates paragraph objects separately from page objects even if it appears that they should be placed in the same location.
- Transparency is not supported when separate graphics items are placed on top of one another. The SCCOPT_EX_PREVENTGRAPHICOVERLAP option does not apply to these

graphics. The graphics will appear relative to where the anchor point is, not relative to the text in the document. Additionally, Dynamic Converter does not support certain graphics effects, such as rotation or stretching.

- It is important to note that the `SCCOPT_EX_GRAPHICOUTPUTDPI` option must be set properly to achieve best results.
- In some cases, Dynamic Converter will produce output with inaccurately placed objects when the input document features positional frame objects. However, this end result is no worse than the end result when handling positional frame objects in pre-7.7 versions of Dynamic Converter (that is, the graphics would be placed in a long column).
- This Element only works in the 4.0 flavors of HTML.

35.16 Template Writing Tips

Given the limited amount of space in each deck, it is important to maximize the amount of usable data in each deck produced by Dynamic Converter. Some ways to reduce the amount of space wasted in each deck include the following:

- Eliminate unnecessary whitespace characters in the template. While the presence of these characters makes reading, editing and maintaining the template easier, they also get written to each output deck "as is." When writing templates for devices with small deck sizes, it may prove worthwhile to remove the extra whitespace characters to increase the amount of usable data in each deck. Please note that the `SCCOPT_EX_COLLAPSEWHITEPSACE` option does not affect white space coming from the template.
- Eliminate any extra links between decks. While good navigation is essential, redundant or unnecessary links eat into the amount of space left in each deck for data. In addition to the markup used for navigation, space is set-aside for the URL of the link, which is determined by the `SCCOPT_EX_MAXURLLENGTH` option. Currently, space is not reclaimed if URLs are shorter than this length. In addition, if URLs are longer than this length, deck overflow may happen.

36
Conversion Filters

This chapter provides information on conversion filters used by Dynamic Converter to convert input files.
This chapter covers the following topics:

- Application Filters
- Graphics Filters

36.1 Application Filters

Dynamic Converter uses the following filters to convert application files (in alphabetical order):

Filter Name	Filter Description
ACD2	AutoCad 2004 /2005 /2006 (text only)
ACS	Microsoft Access 1.0, Microsoft Access 2.0
AMI	Ami Pro, Ami, Professional Write Plus
BDR	Microsoft Office Binder 7.0, Microsoft Office Binder 97 ***(conversion of files contained in the Binder file is supported only on Windows)***
DBS	DBase III, DBase IV, DBase V
DEZ	DataEase 4.x
DIF	Navy DIF
DRW	Micrografx Drawing Products
DX	DEC DX 3.0 and DEC DX 3.1
EMF	Enhanced Windows Metafile
EN4	Enable Word Processor 4.x
ENS	Enable Spreadsheet
ENW	Enable Word Processor 3.0
EXE2	DOS Executable, Windows Executable or DLL
FAX	CCITT Group 3 Fax
FCD	First Choice DB
FCS	First Choice SS
FFT	IBM DCA/FFT
FLW	Freelance 1.0 & 2.0 for OS/2, Freelance 1.0 & 2.0 for Windows, Freelance 96 for Windows 95, Freelance 97 for Windows 95, Freelance for SmartSuite Millennium Edition, Freelance for SmartSuite Millennium Edition 9.6
FWK	Framework III
GDSF	Interface for *.FLT filters (see Graphics Filters)
GIF	CompuServe GIF

Filter Name	Filter Description
GZIP	UNIX GZip
HGS	Harvard Graphics DOS 3.0 Chart, Harvard Graphics DOS 2.0 Chart, Harvard Graphics DOS 3.0 Presentation
HTML	Internet HyperText Markup Language (up to 3.0 with some limitations)
HWP	Hangul 97
HWP2	Hangul 2002
ICH	Ichitaro versions 8.x through 13.x and 2004
ICH6	Ichitaro versions 4.x through 6.x
IWP	Wang IWP
JBG2	JBIG2 graphic embeddings in PDF files
JW	JustWrite 1.0, JustWrite 2.0, Q&A Write 3
LEG	Legacy, Wordstar for Windows
LWP	***For Win32 platforms only.*** Lotus WordPro 96, Lotus WordPro 97, Lotus WordPro for SmartSuite Millennium Edition, Lotus WordPro for SmartSuite Millennium Edition 9.6
LWP7	***For non-Win32 platforms only, and only supporting text extraction/viewing.*** Lotus WordPro 97, Lotus WordPro for SmartSuite for the Millennium, Lotus WordPro for SmartSuite Millennium Edition 9.6
LZH	LZH Compress, LZA Self Extracting Compress
M11	Mass 11
MANU	Lotus Manuscript 1.0, Lotus Manuscript 2.0
MCW	MacWrite II
MIF	FrameMaker MIF versions 3.0, 4.0, 5.0, 5.5 and 6.0 and Japanese 3.0, 4.0, 5.0 and 6.0 (text only)
MIME	MIME-encoded mail messages (See Email Formats for detailed information about MIME support.)
MM	MultiMate 3.6, MultiMate Advantage 2
MM4	MultiMate 4.0
MMFN	MultiMate Note
MP	Multiplan 4
MPP	Microsoft Project versions 98 through 2003 (text only)
MSG	Microsoft Outlook Message and Microsoft Outlook Form Template versions 97, 98, 2000, 2002 and 2003
MSW	Microsoft Word 4.x, Microsoft Word 5.x, Microsoft Word 6.x, Windows Write
MWKD	Mac Works 2.0 Database
MWKS	Mac Works 2.0 Spreadsheet
MWP2	Mac WordPerfect 2.0, Mac WordPerfect 3.0
MWPF	Mac WordPerfect 1.x
MWRK	Mac Works 2.0 WP
OW	OfficeWriter
PCL	PC File 5.0 Doc

Filter Name	Filter Description
PCX	Paintbrush, DCX (multi-page PCX)
PDX	Paradox 2 & 3, Paradox 3.5, Paradox 4, Paradox for Windows
PFS	PFS: Write A, PFS: Write B, Professional Write 1, Professional Write 2, IBM Writing Assistant, First Choice word processor, First Choice 3 word processor
PGL	HP Graphics Language
PIC	Lotus PIC
PICT	Macintosh PICT, Macintosh PICT2
PNTG	MacPaint
PP12	PowerPoint 2007
PP2	Microsoft PowerPoint 3.0 for Windows, PowerPoint 4.0 for Windows, PowerPoint 4.0 for the Mac
PP7	Microsoft PowerPoint 7.0 for Windows 95
PP97	Includes Presentation (PPT) and Slideshow (PPS) support. Microsoft PowerPoint 97, Microsoft PowerPoint Dual 95/97, PowerPoint 98 for the Mac, PowerPoint 2000, PowerPoint 2001 for the Mac, PowerPoint 2002 (XP), PowerPoint 2003, PowerPoint 2004 for the Mac, and PowerPoint v.X for the Mac
PPL	PFS: Plan
PSP6	***For Windows platforms only.*** Paint Shop Pro 5.0 and 6.0
PST	Microsoft Outlook Folder and Microsoft Outlook Offline Folder files versions 97, 98, 2000, 2002 and 2003
PSTF	PST filter support
QA	Q&A Write
QAD	Q&A Database
QP6	Quattro Pro 5.0 - 8.0
QP9	Quattro Pro 9.0 - 12.0 (text only)
RAS	Sun Raster
RBS	R:Base System V, R:Base 5000
RFT	IBM DCA/RFT
RFX	Reflex
RTF	Rich Text Format
SAM	Samna
SC5	SuperCalc 5
SDW	Ami Draw
SHW3	Novell Presentations 3.0, Novell Presentations 7.0, Corel Presentations 8.0 - 12.0, WordPerfect Presentations
SMD	Smart DataBase
SMS	Smart Spreadsheet
SMT	SmartWare II
SNAP	Lotus Snapshot
SOC	StarOffice Calc 5.2 (text only)
SOI	StarOffice Impress 5.2 (text only)

Filter Name	Filter Description
SOW	StarOffice Writer 5.2 (text only)
SPT	Sprint
SWF	Macromedia Flash 6.x, Macromedia Flash 7.x, and Macromedia Flash Lite (text only)
TAZ	UNIX compress, UNIX tar
TEXT	Text - DOS character set, Text - ANSI character set, Text - Macintosh character set, Text - Unicode character set, Text - UTF-8, Text - EBCDIC.
TGA	Truevision TGA (TARGA)
TIF6	Tagged Image File Format, EPS (TIFF header only), CCITT Group 3 Fax, CCITT Group 4 Fax, JPEG, JFIF (JPEG not in TIFF format)
TW	Total Word
TXT	IBM DisplayWrite 2 or 3, IBM DisplayWrite 4, IBM DisplayWrite 5
VCRD	vCard, vCalendar
VISO	Visio 4 - Page Preview mode only (WMF/EMF), Visio 5, 2000, 2002 and 2003
VW3	Volkswriter
W12	Microsoft Word 2007
W6	Microsoft Word 6.0 for Windows, Microsoft Word 7.0 for Windows 95, Microsoft WordPad
W97	Microsoft Word 97, Word 98 for the Mac, Word 98-J, Word 2000, Word 2001 for the Mac, Word 2002 (XP), Word 2003, Word 2004 for the Mac, and Word v.X for the Mac
WG2	Lotus 1-2-3 for OS/2 release 2
WK4	Lotus 1-2-3 3.0, Lotus 1-2-3 4.0, Lotus 1-2-3 5.0
WK6	Lotus 1-2-3 for SmartSuite 97, Lotus 1-2-3 for SmartSuite Millennium Edition, Lotus 1-2-3 for SmartSuite Millennium Edition 9.6
WKS	Lotus 1-2-3 1.0, Lotus 1-2-3 2.0, Symphony, Microsoft Works SS, Microsoft Works DB, VP-Planner, Mosaic Twin, Quattro (DOS), Quattro Pro (DOS), Generic WKS, Windows Works Spreadsheet, Windows Works Database
WM	WordMarc
WMF	Windows Metafile
WORD	Word for Windows 1.x, Word for Windows 2.0, Word for Macintosh 4.0, Word for Macintosh 5.0
WORK	Microsoft Works DOS 1.0 WP, Microsoft Works DOS 2.0 WP, Microsoft Works Win 3.0 WP, Microsoft Works Win 4.0 WP
WP5	WordPerfect 5.x
WP6	WordPerfect 6.0 - 12.0
WPF	WordPerfect 4.2
WPG	WordPerfect Graphic 1.0
WPG2	WordPerfect Graphic 2.0
WPL	Dec WPS Plus 4.1
WPW	Novell PerfectWorks 2.0 word processor, Novell PerfectWorks 2.0 draw, Novell PerfectWorks 2.0 spreadsheet

Filter Name	Filter Description
WS	Wordstar 3.0, Wordstar 4.0, Wordstar 5.0, Wordstar 6.0, Wordstar 7.0
WS2	Wordstar 2000
XL12	Microsoft Excel 2007
XL5	Microsoft Excel 2.x, Excel 3.0, Excel 4.0, Excel 5.0, Excel 7.0, Excel 97, Excel 98 for the Mac, Excel 2000, Excel 2001 for the Mac, Excel 2002 (XP), Excel 2003, Excel 2004 for the Mac, v.X for the Mac, Excel 2.x Chart, Excel 3.0 Chart, Excel 4.0 Chart, Excel 5.0 Chart, Excel 7.0 Chart
XML	XML (text only)
XY	XyWrite /Nota Bene, Signature
YIM	Yahoo! Instant Messenger 6.x and 7.x
ZIP	PKZIP format, self-extracting executable files

36.2 Graphics Filters

Dynamic Converter uses the following filters to convert graphics files (in alphabetical order):

Filter Name	Filter Description
ACAD	AutoCAD Drawing Versions 2.5 - 2.6, 9.0 - 14.0, 2000i and 2002
BMP	Windows Bitmap, Windows Bitmap 98/2000, OS/2 Bitmap, OS/2 Warp Bitmap, Windows Cursor, Windows Icon, Corel Draw 2.0 -11.0
CGM	Computer Graphics Metafile
ESHR	Escher internal Microsoft Office graphics format
IBFPX2.FLT	Kodak Flash Pix
IBGP42.FLT	CALS Raster
IBJPG2.FLT	Progressive JPEG
IBPCD2.FLT	Kodak Photo CD
IBPSD2.FLT	Adobe Photoshop (all versions)
IBXBM2.FLT	X-Windows Bitmap
IBXPM2.FLT	X-Windows Pixmap
IBXWD2.FLT	X-Windows Dump
IMCDR2.FLT IMCD32.FLT IMCD42.FLT IMCD52.FLT IMCD62.FLT IMCD72.FLT IMCD82.FLT	Corel Draw Versions 3, 4, 5, 6, 7, 8
IMCMX2.FLT IMCM52.FLT IMCM72.FLT	Corel Draw Clipart
IMDSF2.FLT	Micrografx Designer Version 6

Filter Name	Filter Description
IMFMV2.FLT	FrameMaker Vector and Raster Graphics (FMV)
IMG	GEM Image (Bitmap)
IMGDF2.FLT	IBM Graphics Data Format (GDF)
IMGEM2.FLT	Gem File (Vector)
IMIGS2.FLT	IGES Drawing
IMMET2.FLT	OS/2 PM Metafile
IMPIF2.FLT	IBM Picture Interchange Format
IMPS_2.FLT IMPSZ2.FLT IMPSI2.FLT	Postscript (Levels 1-2) and EPS files
IMRND2.FLT	AutoShade Rendering
IPHGW2.FLT	Harvard Graphics for Windows
PBM	PBM (Portable Bitmap), PGM (Portable Graymap), PPM (Portable Pixmap)
PDF PDFI	PDF versions 1.0 through 1.6 (including Japanese PDF) and Adobe Illustrator versions 7.0 and 9.0
PNG	Portable Network Graphics

37
Input File Formats

This chapter provides information about the input file formats that Dynamic Converter can process.
This chapter covers the following topics:

37.1 Word Processing Formats

File Format	Comments
ANSI Text	7 & 8 bit
ASCII Text	7 & 8 bit
DEC WPS Plus (DX)	Versions through 3.1
DEC WPS Plus (WPL)	Versions through 4.1
DisplayWrite 2 & 3 (TXT)	All versions
DisplayWrite 4 & 5	Versions through 2.0
EBCDIC	All versions
Enable	Versions 3.0, 4.0 and 4.5
First Choice	Versions through 3.0
Framework	Version 3.0
Hangul	Versions 97 – 2010
IBM DCA/FFT	All versions
IBM Writing Assistant	Version 1.01
Just System Ichitaro	5.0, 6.0, 8.0 –13.0, 2004, 2010
JustWrite	Versions through 3.0
Kingsoft WPS Writer	2010
Legacy	Versions through 1.1
Lotus Manuscript	Version 2.0

File Format	Comments
Lotus Word Pro (non-Windows)	Versions SmartSuite 97, Millennium, and Millennium 9.6 (text only)
Lotus Word Pro (Windows)	Versions SmartSuite 96, 97 and Millennium and Millennium 9.6
MacWrite II	Version 1.1
MASS11	Versions through 8.0
Microsoft Rich Text Format (RTF)	All versions
Microsoft Word (DOS)	Versions through 6.0
Microsoft Word (Mac)	Versions 4.0 - 2004
Microsoft Word (Windows)	Versions through 2007
Microsoft WordPad	All versions
Microsoft Works (DOS)	Versions through 2.0
Microsoft Works (Mac)	Versions through 2.0
Microsoft Works (Windows)	Versions through 4.0
Microsoft Windows Write	Versions through 3.0
MultiMate	Versions through 4.0
Navy DIF	All versions
Nota Bene	Version 3.0
Novell Perfect Works	Version 2.0
Novell/Corel WordPerfect (DOS)	Versions through 6.1
Novell/Corel WordPerfect (Mac)	Versions 1.02 through 3.0
Novell/Corel WordPerfect (Windows)	Versions through 12.0
Office Writer	Versions 4.0 - 6.0
PC-File Letter	Versions through 5.0
PC-File+ Letter	Versions through 3.0
PFS:Write	Versions A, B and C
Professional Write (DOS)	Versions through 2.1
Professional Write Plus (Windows)	Version 1.0
Q&A (DOS)	Version 2.0
Q&A Write (Windows)	Version 3.0
Samna Word	Versions through Samna Word IV+
Signature	Version 1.0
SmartWare II	Version 1.02
Sprint	Versions through 1.0
StarOffice Writer	Version 5.2 (text only) and 6.x through 8.x
Total Word	Version 1.2
Unicode Text	All versions
UTF-8	All versions
Volkswriter 3 & 4	Versions through 1.0

File Format	Comments
Wang PC (IWP)	Versions through 2.6
WordMARC	Versions through Composer Plus
WordStar (DOS)	Versions through 7.0
WordStar (Windows)	Version 1.0
WordStar 2000 (DOS)	Versions through 3.0
XHTML (file ID only)	1.0
XML (text only)	All versions
XyWrite	Versions through III Plus

37.2 Desktop Publishing Formats

File Format	Comments
Adobe FrameMaker (MIF)	Versions 3.0, 4.0, 5.0, 5.5 and 6.0 and Japanese 3.0, 4.0, 5.0 and 6.0 (text only)

37.3 Database Formats

File Format	Comments
dBASE	Versions through 5.0
DataEase	Version 4.x
First Choice DB	Versions through 3.0
Framework DB	Version 3.0
Microsoft Works (Windows)	Versions through 4.0
Microsoft Works (DOS)	Versions through 2.0
Microsoft Works (Mac)	Versions through 2.0
Paradox (DOS)	Versions through 4.0
Paradox (Windows)	Versions through 1.0
Personal R:BASE	Version 1.0
R:BASE 5000	Versions through 3.1
R:BASE System V	Version 1.0
Reflex	Version 2.0
Q & A	Versions through 2.0
SmartWare II	Version 1.02

37.4 Spreadsheet Formats

File Format	Comments
Apple iWork Numbers	09
Enable	Versions 3.0, 4.0 and 4.5
First Choice	Versions through 3.0
Framework	Version 3.0
Lotus 1-2-3 (DOS & Windows)	Versions through 5.0
Lotus 1-2-3 (OS/2)	Versions through 2.0
Lotus 1-2-3 Charts (DOS & Windows)	Versions through 5.0
Lotus 1-2-3 for SmartSuite	Versions 97 - Millennium 9.6
Lotus Symphony	Versions 1.0, 1.1 and 2.0
Microsoft Excel Charts	Versions 2.x - 7.0
Microsoft Excel (Mac)	Versions 3.0 –4.0, 98, 2001, 2002, 2004, and v.X
Microsoft Excel (Windows)	Versions 2.2 through 2007
Microsoft Multiplan	Version 4.0
Microsoft Works (Windows)	Versions through 4.0
Microsoft Works (DOS)	Versions through 2.0
Microsoft Works (Mac)	Versions through 2.0
Novell Perfect Works	Version 2.0
PFS:Professional Plan	Version 1.0
Quattro Pro (DOS)	Versions through 5.0 (text only)
Quattro Pro (Windows)	Versions through 12.0 (text only)
SmartWare II	Version 1.02
SuperCalc 5	Version 4.0
VP Planner 3D	Version 1.0

37.5 Presentation Formats

File Format	Comments
Apple iWork Keynote	09
Harvard Graphics (DOS)	Versions 2.x & 3.x
Harvard Graphics (Windows)	Windows versions
IBM Lotus Symphony	Version 1.x
Kingsoft WPS	2010
Freelance (Windows)	Versions through Millennium 9.6
Freelance (OS/3)	Versions through 2.0
Microsoft PowerPoint (Windows)	Versions 3.0 through 2007
Microsoft PowerPoint (Mac)	Versions 4.0 through v.X

File Format	Comments
Microsoft PowerPoint (Windows slideshow/template)	2007–2013
Novell Presentations	Versions through 12.0
WordPerfect	5.1–X

37.6 Graphic Formats

File Format	Comments
Adobe Photoshop (PSD)	All versions
Adobe Illustrator	Versions 7.0 and 9.0
Adobe FrameMaker graphics (FMV)	Vector/raster through 5.0
Adobe Acrobat (PDF)	Versions 1.0, 2.1, 3.0, 4.0, 5.0, 6.0 and 7.0 (including Japanese PDF)
Ami Draw (SDW)	Ami Draw
AutoCAD Interchange and Native Drawing formats (DXF and DWG)	AutoCAD Drawing Versions 2.5 - 2.6, 9.0 -14.0, 2000i and 2002
AutoShade Rendering (RND)	Version 2.0
Binary Group 3 Fax	All versions
Bitmap (BMP, RLE, ICO, CUR, OS/2 DIB & WARP)	All versions
CALS Raster (GP4)	Type I and Type II
Corel Clipart format (CMX)	Versions 5 through 6
Corel Draw (CDR)	Versions 3.x - 8.x
Corel Draw (CDR with TIFF header)	Versions 2.x - 11.0
Computer Graphics Metafile (CGM)	ANSI, CALS NIST version 3.0
Encapsulated PostScript (EPS)	TIFF header only
GEM Paint (IMG)	All versions
Graphics Environment Mgr (GEM)	Bitmap & vector
Graphics Interchange Format (GIF)	All versions
Hewlett Packard Graphics Language (HPGL)	Version 2
IBM Graphics Data Format (GDF)	Version 1.0
IBM Picture Interchange Format (PIF)	Version 1.0
Initial Graphics Exchange Spec (IGES)	Version 5.1
JBIG2	JBIG2 graphic embeddings in PDF files
JFIF (JPEG not in TIFF format)	All versions
JPEG (including EXIF)	All versions
Kodak Flash Pix (FPX)	All versions
Kodak Photo CD (PCD)	Version 1.0
Lotus PIC	All versions

File Format	Comments
Lotus Snapshot	All versions
Macintosh PICT1 & PICT2	Bitmap only
MacPaint (PNTG)	All versions
Micrografx Draw (DRW)	Versions through 4.0
Micrografx Designer (DRW)	Versions through 3.1
Micrografx Designer (DSF)	Windows 95, version 6.0
Novell PerfectWorks (Draw)	Version 2.0
OS/2 PM Metafile (MET)	Version 3.0
Paint Shop Pro 6 (PSP)	Windows only, versions 5.0 - 6.0
PC Paintbrush (PCX and DCX)	All versions
Portable Bitmap (PBM)	All versions
Portable Graymap (PGM)	No specific version
Portable Network Graphics (PNG)	Version 1.0
Portable Pixmap (PPM)	No specific version
Postscript (PS)	Levels 1-2
Progressive JPEG	No specific version
Sun Raster (SRS)	No specific version
TIFF	Versions through 6
TIFF CCITT Group 3 & 4	Versions through 6
Truevision TGA (TARGA)	Version 2
Visio (preview)	Version 4
Visio	Versions 5, 2000, 2002 and 2003
WBMP	No specific version
Windows Enhanced Metafile (EMF)	No specific version
Windows Metafile (WMF)	No specific version
WordPerfect Graphics (WPG & WPG2)	Versions through 2.0
X-Windows Bitmap (XBM)	x10 compatible
X-Windows Dump (XWD)	x10 compatible
X-Windows Pixmap (XPM)	x10 compatible

37.7 Compressed Formats

File Format	Comments
LZA Self Extracting Compress	
LZH Compress	
Microsoft Binder	Versions 7.0-97 ***(conversion of files contained in the Binder file is supported only on Windows)***
UUEncode	

File Format	Comments
UNIX Compress	
UNIX GZIP	
UNIX TAR	
ZIP	PKWARE versions through 2.04g

37.8 Email Formats

File Format	Comments
Apple Mail Message	2.0
Encoded mail messages	MHT, Multi Part Alternative, Multi Part Digest, Multi Part Mixed, Multi Part News Group, Multi Part Signed, and TNEF
EML/MSG with digital signature	SMIME
IBM Lotus Notes (Domino XML language DXL, NSF FileID, NSF)	7.x, 8.x, and 8.5
MBOX mailbox	RFC 822
Microsoft Outlook Folder (PST)	Microsoft Outlook Folder and Microsoft Outlook Offline Folder files versions 97, 98, 2000, 2002 and 2003
Microsoft Outlook Message (MSG)	Microsoft Outlook Message and Microsoft Outlook Form Template versions 97, 98, 2000, 2002 and 2003
MIME	MIME-encoded mail messages. (See below for detailed information about MIME support.)

MIME Support Notes

Here is detailed information about support for MIME-encoded mail message formats.

- MIME formats, including:
  - EML
  - MHT (Web Archive)
  - NWS (Newsgroup single-part and multi-part)
  - Simple Text Mail (defined in RFC 2822)
- TNEF Format
- MIME encodings, including:
  - base64 (defined in RFC 1521)
  - binary (defined in RFC 1521)
  - binhex (defined in RFC 1741)
  - btoa
  - quoted-printable (defined in RFC 1521)
  - utf-7 (defined in RFC 2152)
  - uue

- xxe
- yenc

Additionally the body of a message can be encoded several ways. We support the following encodings:

- Text
- HTML
- RTF
- TNEF
- Text/enriched (defined in RFC1523)
- Text/richtext (defined in RFC1341)
- Embedded mail message (defined in RFC 822). This is handled as a link to a new message.

> **Note:**
>
> The attachments of a MIME message can be stored in many formats. All attachments of supported file formats can be converted.

37.9 Other Formats

File Format	Comments
AOL Messenger	7.3
Executable (EXE, DLL)	
HTML	Versions through 3.0, with some limitations
MacroMedia Flash	Macromedia Flash 6.x, Macromedia Flash 7.x, and Macromedia Flash Lite (text only)
Microsoft Project	Versions 98 through 2003 (text only). (MPP files are treated as database files.)
vCard, vCalendar	Version 2.1
Windows Executable	
XML	Text only
Yahoo! Instant Messenger	Versions 6.x and 7.x

38
Office 2007/2010 Considerations

This chapter provides a number of considerations related to dynamic conversion of Office 2007/2010 files.
This chapter covers the following topics:

38.1 All Office Applications

Please note the following conversion limitations that currently apply for all Office 2007/2010 applications:

- Smart art in pre-Office 2007 SP2 (released in April 2009) (see Examples of Unsupported Objects for an example)
- VB controls and macros (see Examples of Unsupported Objects for an example)
- Table cell formatting
- Word art (see Examples of Unsupported Objects for an example)
- Vector graphics (Office art & VML) transparency, picture styles, effects, etc. (see Examples of Unsupported Objects for an example)
- Password-protected documents

38.2 Word 2007/2010

Please note the following conversion limitations that currently apply for Word 2007/2010 documents:

- Picture bullets
- Tint support
- List level overrides
- OLE objects
- Equations (see Examples of Unsupported Objects for an example)
- Theme effects (in Office art)
- Line numbers
- Watermarks
- Page color (not supported in the viewer)

- Footnote and end note reference numbers
- Revision delete attributes (text is supported)
- Controls (only last edited text is output for legacy controls)
- Custom XML (structure, schemas, expansion packs), cfChunk/altChunks are not supported

38.3 Excel 2007/2010

Please note the following conversion limitations that currently apply for Excel 2007/2010 spreadsheets:

- Conditional formatting (highlight cells with rules, top bottom rules, data bars, color scale icon sets, and custom rules; see Examples of Unsupported Objects for an example).
- Formatting as tables (the data in the cell is output, but the formatting is not retained)
- Headers and footers (different even/odd page headers are not supported)

38.4 PowerPoint 2007/2010

Please note the following conversion limitations that currently apply for PowerPoint 2007/2010 presentations:

- Table formatting (similar to Excel)
- Actions are currently not supported
- "Objects" (this is represented as VML; currently not supported)
- Movies/sounds are not supported
- Complex gradients are not supported (see Examples of Unsupported Objects for an example)
- Animation is currently not supported
- Only solid fills are supported for text
- Only left-to-right text direction is supported (not related to bi-directional)
- Shading and fills of certain shapes are not supported (see Examples of Unsupported Objects for an example)
- Transparency of lines/vector objects is not supported

38.5 Examples of Unsupported Objects

This section provides some examples of Office 2007/2010 objects that cannot be converted at this point.

Figure 38-1 Smart Art

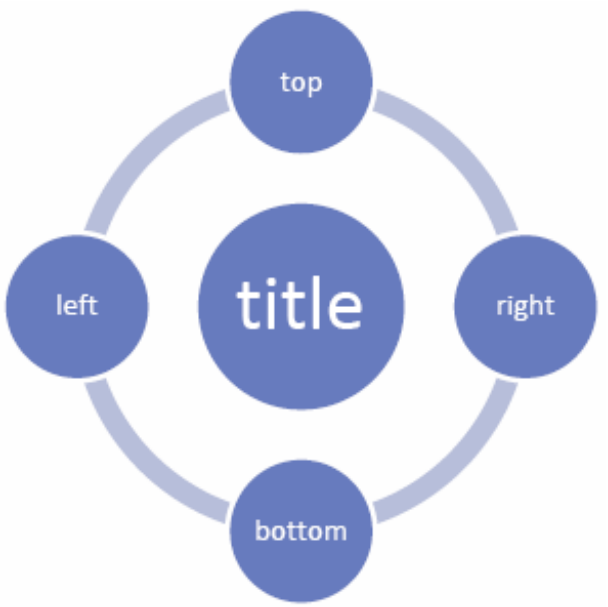


Figure 38-2 Picture Styles and Effects

Figure 38-3 Word Art

Figure 38-4 Equations

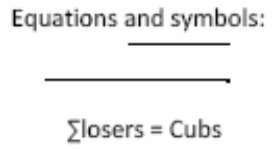


Figure 38-5 Controls

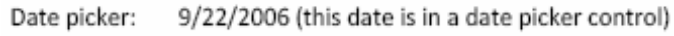


Figure 38-6 Data Bars with Conditional Formatting, Color Scales, and Icon Sets

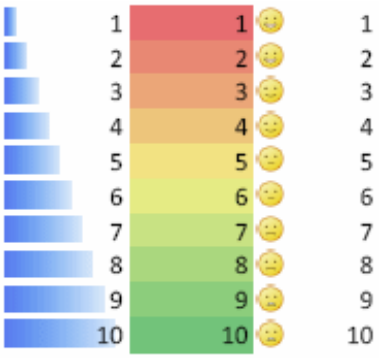


Figure 38-7 3D Effects in PowerPoint

Figure 38-8 Complex Gradients

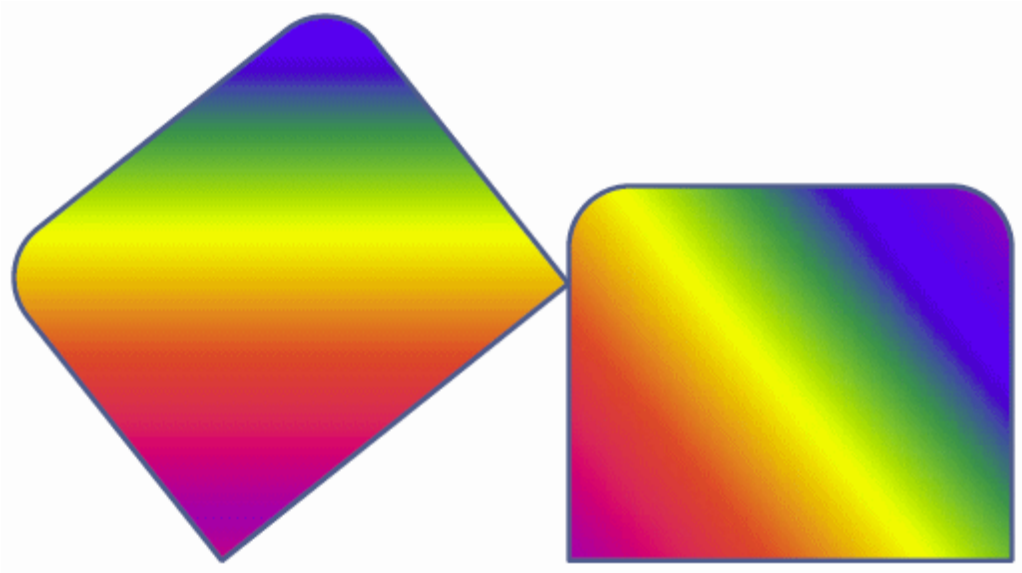
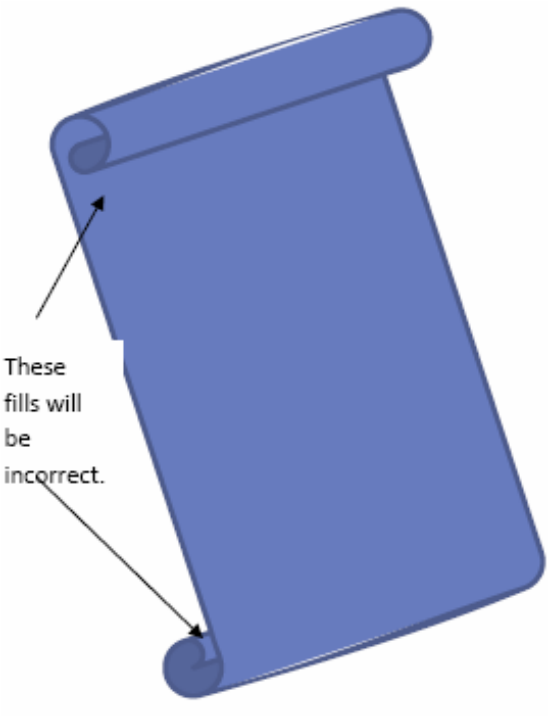


Figure 38-9 Complex Shapes with Varying Fills (1)

Figure 38-10 Complex Shapes with Varying Fills (2)



Part VII
Desktop Management

This part provides information on managing Oracle WebCenter Content: Desktop.

Desktop Management contains the following chapter:

- Managing Desktop

39
Managing Desktop

This chapter provides information on managing Oracle WebCenter Content: Desktop, which provides a set of embedded applications that help to seamlessly integrate users' desktop experience with Oracle WebCenter Content, Oracle WebCenter Content Server, Oracle Content Database, or other WebDAV-based content repositories.
For information about using Desktop, see *Using Oracle WebCenter Content: Desktop*.

This chapter covers these topics:

39.1 Custom Installation Options for the Client Software

The Desktop client software installers support a number of custom installation options that can help system administrators roll out the software:

- Command-line operation: You can use a number of command-line parameters to automate (part of) the installation process.
- Disabling integrations: The Desktop installers provide a number of command-line options that enable you to disable specific software integrations.
- Silent roll-outs: The MSI installer enables the system administrator to roll out the Desktop client software to multiple client machines with the help of third-party tools such as SMS or netOctopus, which are capable of executing one executable on many machines.

For information on using these options, see Extracting and Running the Installation File for Client Desktop Software in *Installing and Configuring Oracle WebCenter Content*.

39.2 Setting the Web Browser Search Provider Name for a Content Server Instance

Desktop provides plug-ins for various popular web browsers which enable users to search for content on a Content Server instance directly from the search field in their web browser. For more information about the search provider web browser plug-in, see *Using Oracle WebCenter Content: Desktop*.

The default search provider name for a Content Server instance is `Oracle WebCenter Content Search`, but this can be modified to a more meaningful name for the server.

To modify the default search provider name:

1. Log in to Content Server as an administrator.
2. Open the **Administration** tray or menu and choose **Configuration for *Server***.
3. On the Configuration Information for *Server* page, under **Features And Components**, click **Enabled Component Details**.
4. In the list of all installed components, find **DesktopIntegrationSuite** and click its **Configure** link.
5. On the Update Component Information page, make sure the **Enable web browser search plug-in** check box is selected.
6. Enter the search provider name for the server in the **Web browser search plug-in title** field.

> **Note:**
>
> Make sure to choose a search provider name that is unique across your organization. You cannot have two servers with the same search provider name.

7. When you are done, click **Update** to enable the new settings, **Reset** to cancel any modifications, or **Revert To Install Settings** to return to all default settings.
8. Restart the Content Server instance.

If a user hasn't logged in to the Content Server, the user's search with the web browser is performed anonymously and returns only content that is available to the guest role. To make sure the search is performed as the authenticated user, the extra parameter `Auth=Internet` can be passed to the Content Server to cause the service to challenge the search request and force a login if needed.

Because the definition of the search engine URL is defined within the DesktopIntegrationSuite component, a new custom component can be added to override this, forcing authentication. Essentially the new component must override the `dis_search_plugin` resource and modify the Url locations. For an example of custom code and a sample component, see the "Adding Browser Search Engines in WebCenter Content" blog.

39.3 Enabling Subfolder Searching

If a Content Server 12*c* instance is using Framework Folders as the content hierarchy component, then you can enable subfolder searching. This allows users to specify whether a content search should apply to the current folder only or whether it should include all subfolders of that folder.

To enable subfolder searching, the Content Server instance must be configured to use the Oracle Text Search engine and some elements must be added to the search form.

To enable subfolder searching:

1. Log in to Content Server as an administrator.

2. Open the **Administration** tray or menu and choose **Admin Server**, then choose **General Configuration**.
3. On the General Configuration page, make sure the **Additional Configuration Values** section includes the following entries:

   ```
   SearchIndexerEngineName=OracleTextSearch
   FoldersIndexParentFolderValues=true
   ```

4. Click **Save**.
5. Restart the Content Server instance.
6. Rebuild the search collection index using the Repository Manager utility.

The content search form now includes a **Parent Folder** field as well as an **Include Subfolders** check box, which allows users to limit a search query to just the current content folder or expand it to include all subfolders.

39.4 Mapping Email Metadata

System administrators can map email header fields to metadata fields for email messages that are checked in to the Content Server. This is done on the Map MSG Metadata and Map EML Metadata pages, which are available in the Content Server web interface. MSG metadata mapping is used for the Microsoft Outlook message format and EML metadata mapping for Internet mail message format.

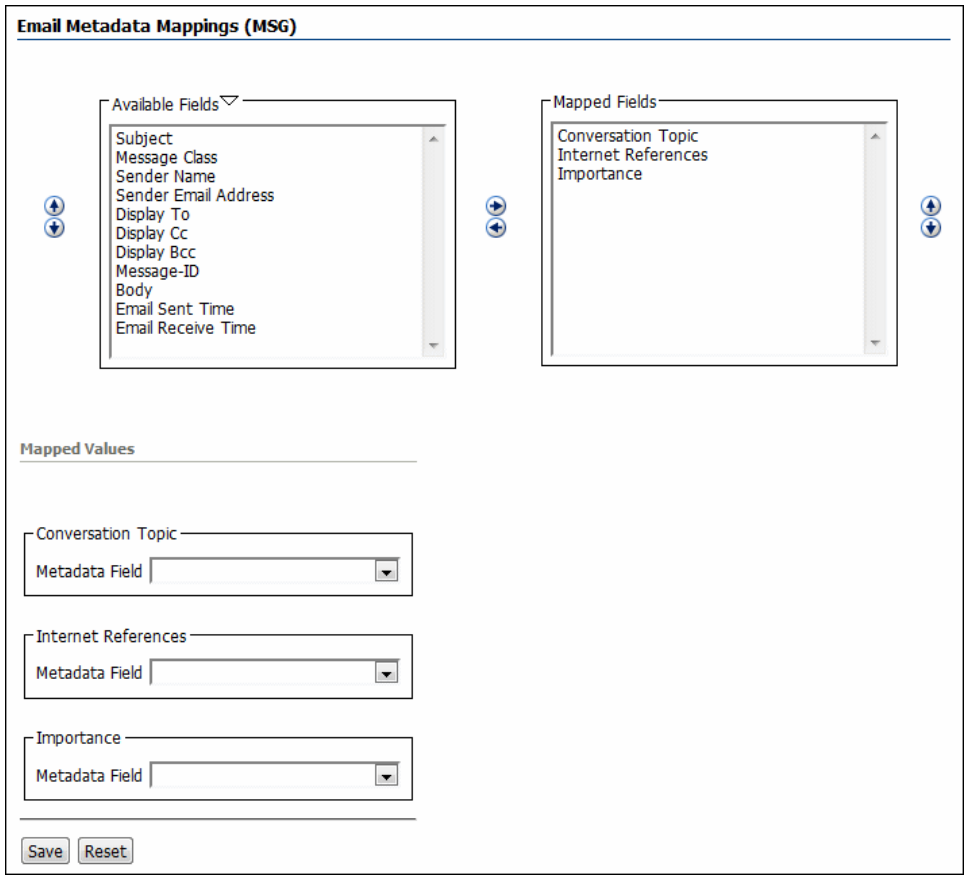
Please note that you cannot override the six standard email metadata mappings; you can only create additional mappings. (See *Using Oracle WebCenter Content: Desktop*.)

To map email metadata:

1. Log in to Content Server as an administrator.
2. Open the **Administration** tray or menu and choose **Configure Email Metadata** and then **Map MSG Metadata** or **Map EML Metadata**.

   The Email Metadata Mappings page displays (MSG or EML) (see Figure 39-1).
3. The email header fields listed under **Available Fields** are not mapped to Content Server metadata fields. The fields listed under **Mapped Fields** are mapped to metadata. Use the right and left arrows to select a field and move it from one group to the other. Use the up and down arrows to sort the fields within each grouping.
4. As fields are added to or removed from **Mapped Fields**, a drop-down list appears for that field under **Mapped Values**. For each mapped email header field, select a value for the metadata field from the drop-down list.
5. Once all fields have been updated with metadata values, click **Save**.

Figure 39-1 Email Metadata Mappings (MSG) Page



Element	Description
Available Fields	The email header fields in this list can be mapped to Content Server metadata fields. Use the up and down arrows to sort the fields, and once a field is selected, use the right arrow to move it into the Mapped Fields box.
Mapped Fields	The email header fields in this list are mapped to Content Server metadata fields. Use the up and down arrows to sort the fields, and once a field is selected, use the left arrow to move it into the Available Fields box (and unmap the field).
Mapped Values	Each email header field in the Mapped Fields list is included in this area. Select a Content Server metadata field in the drop-down list to map the email header field to.
Save	Saves the email mapping information on the server.
Reset	Resets all fields to their values when the screen was opened in this session.

39.5 Configuring Form-Based Login

Your organization may use separate identity and access management software that provides secure, form-based login screens to authenticate users and control what they have access to on the network. Desktop is compatible with form-based logins. To set

this up, system administrators need to add a comment to the login page so that Desktop identifies an HTML response as the forms-based login page. Users, as a result, will see the form-based login instead of the standard Oracle WebCenter Content Server login.

To configure form-based login:

1. Locate the login form on the file system (for example, `login.fcc` for Netegrity SiteMinder). The location of this form depends on how the authentication system was set up in your organization.
2. Open the form in a text editor.
3. Add the following comment (with no spaces) to the HEAD section of the form:

   ```
   <!--IdcClientLoginForm=1-->
   ```

   > **Note:**
   >
   > The form's HEAD section may contain a lot of code; for example, many META tags or JavaScript code. The delivered page must have that HTML comment (or token) in the first 5,000 characters of the response, otherwise the server connection may fail. The software on the client computer seeks the response for the `<!--IdcClientLoginForm=1-->` token (using a strict string search) and route through the prompting code if it is found. It is encoded as an HTML comment so that regular browsers do not show the token when they attempt to log in. (If it is Idoc Script, then the parser removes that bit of code from the delivered page, and the client-side browser will not see anything in the page.)

4. Save and close the form.

The next time users connect to a Content Server instance using Desktop, they will see a login form, where they can provide their user name and password to log on.

39.6 Customizing the Form-Based Login Regular Expression

By default, Desktop 12*c* uses the following regular expression to identify a form-based login:

```
<!--IdcClientLoginForm=1-->|
<form .*sso.* name=\"LoginForm\"|
<form *name=\"loginForm\"
```

This regular expression is configurable in the Windows Registry. The code first looks in the following place:

```
[HKEY_LOCAL_MACHINE\SOFTWARE\Oracle\Universal Content Management\Desktop Integration
Suite\WebDAV\Servers\SERVER_NAME]
"Form Based Logins Reg Exp"="REGULAR_EXPRESSION"
```

Then in:

```
[HKEY_CURRENT_USER\SOFTWARE\Oracle\Universal Content Management\Desktop Integration
Suite\WebDAV\Servers\SERVER_NAME]
"Form Based Logins Reg Exp"="REGULAR_EXPRESSION"
```

Then in:

```
[HKEY_LOCAL_MACHINE\SOFTWARE\Oracle\Universal Content Management\Desktop
Integration Suite\WebDAV]
"Form Based Logins Reg Exp"="REGULAR_EXPRESSION"
```

And finally in:

```
[HKEY_CURRENT_USER\SOFTWARE\Oracle\Universal Content Management\Desktop
Integration Suite\WebDAV]
"Form Based Logins Reg Exp"="REGULAR_EXPRESSION"
```

If no custom regular expression is defined in any of these Windows Registry locations, the default one is used.

39.7 Setting the Naming of Files for Checked-In Email Messages

When checking in an email message, a file name is used to identify that message on the content server. The default is to base the file name on the subject line (Lotus Notes) or a combination of the subject line and the date received (Microsoft Outlook). For Microsoft Outlook, other attributes of the email message can be used for the file name by setting a registry key. (See Configuring and Disabling Pattern-based File Naming for Email Check-ins in *Using Oracle WebCenter Content: Desktop*.)

An alternative method of generating file names is available. This will always use the subject line, the internet message ID, or the GUID, as available and appropriate. To use this method, a normally unselected option on a configuration page must be selected.

To use the alternative method of file naming:

1. Log in to Content Server as an administrator.
2. Open the **Administration** tray or menu and choose **Configuration for *Server***.
3. On the Configuration Information for *Server* page, under **Features And Components**, click **Enabled Component Details**.
4. In the list of all installed components, find **EmailMetadata** and click its **Configure** link.
5. On the Email Metadata Component page, make sure the **Set file name to e-mail subject line if title identical to file name** check box is selected.
6. When you are done, click **Update** to enable the new settings, **Reset** to cancel any modifications, or **Revert To Install Settings** to return to all default settings.
7. Restart the Content Server instance.

39.8 Enabling Related Content Links for Checked-In Email Attachments

Email client integration enables you to check email messages and their attachments in to a content server directly from Microsoft Outlook or Lotus Notes. When users check email messages with attachments in to the content server, they can set an option in the desktop client to check in an attachment separately from its email message. This

feature leverages the Related Content component to enable users to create cross-references between the email and its attachments

Part VIII
Troubleshooting

This part of the documentation discusses troubleshooting options for some Oracle WebCenter Content applications.

Troubleshooting contains the following chapters:

- Troubleshooting Workflows
- Troubleshooting Content Tracking Issues
- Troubleshooting WebDAV
- Troubleshooting Inbound Refinery

40
Troubleshooting Workflows

Workflows are used to specify how content is routed for review, approval, and release to the system. This chapter provides solutions to several common workflow issues.
This chapter discusses the following topics:

40.1 Workflow Item Stuck in EDIT or GENWWW Status

Symptom

A content item in a workflow is in EDIT or GENWWW status, and no reviewers were notified by email that action is required.

Problem

Inbound Refinery failed to convert the file properly.

Recommendation

1. View the content item's status in Repository Manager or the Content Items for Workflow page (accessed from **Content Manager**, then **Active Workflows** then *Workflow_Name*). For information about the conversion failure, display the Content Information page.
2. Determine why the conversion failed:
   - If the problem was with Inbound Refinery or a conversion component:
     a. Correct the problem so that the file converts properly.
     b. Resubmit the file for conversion from Repository Manager or Content Information page. The content item continues through the workflow.
   - If the problem was with a file in a criteria workflow and the content item is the only item in the workflow:
     a. Save a copy of the native file.
     b. Disable the workflow to release the content item.
     c. Delete the released revision using Repository Manager or the Content Information page.
     d. Correct the problem so that the file converts properly.
     e. Check in the content item again so that it goes through the entire workflow process.
   - If the problem was with a file in a criteria workflow and there are multiple content items in the workflow:
     a. Save a copy of the native file.

b. Delete the "stuck" revision using Repository Manager. (You could disable the workflow, but all content items in the workflow would be released.)

c. Correct the problem so that the file converts properly.

d. Check in the content item again so that it goes through the entire workflow process

- If the problem was with a file in a basic workflow and the content item is the only item in the workflow:

  a. Save a copy of the native file.

  b. Cancel the workflow to delete the revision from the system.

  c. Correct the problem so that the file converts properly.

  d. Contribute the content item again to the Basic workflow so that it goes through the entire workflow process.

- If the problem was with a file in a basic workflow and there are multiple content items in the workflow:

  a. Save a copy of the native file.

  b. Delete the "stuck" revision using Repository Manager. (You could cancel the workflow, but all content items in the workflow would be deleted from the system.)

  c. Correct the problem so that the file converts properly.

  d. Contribute the content item again to the Basic workflow so that it goes through the entire workflow process

40.2 Workflow Item Stuck in REVIEW Status

Symptom

A content item in a workflow is in REVIEW status, and the minimum number of reviewers have approved it, but the revision is not moving to the next step.

Problem

The content item does not meet the exit criteria of the workflow.

Recommendation

1. Check the exit condition definition in the workflow step to see why the document does not meet the criteria.
2. Determine if the file is finished interacting with an external process. Resolve any problems with the external process to see if the file meets the exit condition.
3. If there is an error in the exit condition, external processing or both, you can check out the document and check it back in with the correct metadata to meet the exit condition.

40.3 Workflow Item Entered in Wrong Workflow

Symptom

A content item entered the wrong criteria workflow.

Problem

Two or more criteria workflows have the same criteria defined. The content item matched this criteria, so it entered the first matching workflow in the workflow list.

Recommendation

Redefine the criteria so that each workflow has a unique combination of the security group and metadata field value. If necessary, use jumps and sub-workflows to define additional criteria within the main workflow.

41
Troubleshooting Content Tracking Issues

Content Tracker has two execution trace mechanisms: the Web server filter plug-in and the Java code. These are intended for diagnosing problems at customer installations and are not to be used in production.
Hanging browser: If Content Server terminates while the Data Engine Control Center is running, the browser can also hang. To resolve the issue, close the browser window.

This chapter includes the following topics:

41.1 Web Server Filter Plug-in Debugging Support

The Web server filter plug-in honors `PLUGIN_DEBUG`. Enable `PLUGIN_DEBUG` on the Filter Administration page and the Content Tracker Web server filter plug-in issues execution trace information. The trace is only meaningful to someone with access to the source. Customers with a problem are expected to enable `PLUGIN_DEBUG`, run the test scenario, then send the log segments to Customer Service for evaluation. Otherwise, turn `PLUGIN_DEBUG` off.

To set PLUGIN_DEBUG:

1. Choose **Administration** then **Admin Applets** from the Main menu.
2. Click **Filter Administration**.
3. On the Configure Web Server Filter Plug-in page, select PLUGIN_DEBUG.
4. Click **Update**.

41.2 Java Code Debugging Support

Use the System Audit functionality in Content Server for debugging support. For more information, see System Audit Information in *Administering Oracle WebCenter Content*. Add `contenttracker` to the Active Sections list. When the list is updated, the Content Tracker execution trace information appears with the other active sections.

41.3 DataBinder Dump Facility

When Content Tracker records a specific service in the log file, it records the contents of the service's DataBinder object in a serialized dump file. The contents of these files are useful for debugging field maps that use the extended service call tracking function. These dump files allow you to see the available LocalData fields for the recorded service.

The Content Tracker service handler filter only creates dump files for DataBinder objects if the associated services are defined in the `SctServiceFilter.hda` file.

> **Caution:**
>
> The dump files for DataBinder objects continue to accumulate until manually deleted. Use the `SctDebugServiceBinderDumpEnabled` configuration variable only as necessary.

Set the `SctDebugServiceBinderDumpEnabled` configuration variable to true to configure the service handler filter to write out the objects into dump files. For more information about Tracker Configuration variables, see *Configuration Reference for Oracle WebCenter Content*.

The files are stored in the `/ContentTracker/DEBUG_BINDERDUMP` directory. File names consist of three parts: *`service_name_filter_function_serial_number`*`.hda`

- *service_name* is the name of the logged service (such as, GET_FORM_FILE).
- *filter_function* is one of the following:
  - End: Filter Event on EndServiceRequestActions. Normal end-of-service event.
  - EndSub: FilterEvent on EndScriptSubServiceActions. Normal end-of-service for service called as SubService.
  - Error: Filter Event on ServiceRequestError. End of service where an error occurred. Can happen in addition to End.
- *serial_number* is the unique identification number assigned to the file. Content Tracker can create multiple DataBinder object dump files for a given service.

Example:

```
GET_SEARCH_RESULTS_End_1845170235.hda
```

42
Troubleshooting WebDAV

This chapter describes troubleshooting with WebDAV.

> **Tip:**
>
> For error messages and information about the operation of the WebDAV component, see the Content Server logs.

This chapter contains the following topics:

42.1 Zero-Byte Files

When using an Office 2000 application to open a document that resides on a WebDAV server, the application displays the content as empty (0 bytes).

42.1.1 Cause

This problem can be caused by a combination of the temporary Internet files settings in Microsoft Internet Explorer. The WebDAV file is still present in Content Server, but does not open properly on certain client computers with particular settings.

42.1.2 Solution

1. In Internet Explorer, select **Tools** then **Internet Options**.
2. On the **General** tab, click **Settings**.
3. Under "Check for newer versions of stored pages," select **Every visit to the page**.

4. Under "Temporary Internet files folder," consider increasing the amount of disk space. (The lower the amount, the sooner the empty file problem seems to occur.)
5. Click **OK** twice to save the settings and close the page.

42.2 No Connection to WebDAV Folder

A client computer does not connect to WebDAV folders.

42.2.1 Cause

Internet Explorer is configured to use a proxy server.

42.2.2 Solution

Do one of the following:

- Configure the client computer to not use the proxy server instance for your HTTP server/WebDAV server. To do this in Internet Explorer, select **Tools** then **Internet Options**. Select **Connections** then **LAN Settings** then **Advanced** then **Exceptions**. Specify the IP address/host name of the WebDAV server.
- Modify the proxy server configuration to allow pass-through for WebDAV methods (WebDAV-specific HTTP/1.1 extensions) with standard GET, POST, and other HTTP/1.1 methods. For more information, see your proxy server documentation.
- Windows Vista requires Service Pack 2 for WebDAV to work properly.

42.3 Other Connection Issues

- Some versions of Windows XP, Vista, and 7 do not connect to a WebDAV server running over HTTP and using HTTP Basic authentication. You must set a registry entry to fix this. For more information, see `http://support.microsoft.com/kb/841215`.
- When mapping a network drive in Windows 7, Windows remembers all failed attempts in a login session and never retries a connection after a single connection to a host has failed, even if the browser cache is cleared in Internet Explorer and you modify the WebDav URL. To work around this issue, restart Windows 7 before trying to connect to that host again through WebDAV.
- By default, Office 2010 will not open documents over WebDAV using basic authentication over a non-SSL connection. You must set a registry entry to fix this. For more information, see `http://support.microsoft.com/kb/2123563`.

42.4 Double-Byte Characters in File Name

A file with double-byte characters in the file name cannot be checked in.

42.4.1 Cause

If the Content Server is running on a Western European operating system, the Microsoft WebDAV client may not be able to handle files with double-byte characters in the file name.

42.4.2 Solution

Either eliminate all double-byte characters from the file name, or check in the file through the Content Server's Web browser interface.

42.5 Number Sign in Virtual Folder Name or File Name

Using the number sign (#) in a folder name generates errors and truncates the folder name before the number sign. Using the number sign (#) in file names generates errors.

42.5.1 Cause

The number sign (#) is not allowed in WebDAV folder or file names.

42.5.2 Solution

Eliminate the number sign (#) from the folder name. Either eliminate the number sign from the file name, or check in the file through the Content Server's Web browser interface.

42.6 ExtranetLook Component Problem

The ExtranetLook component no longer works after installation of the Folder component.

42.6.1 Cause

The WebDAV component uses CookieLoginPlugin.dll for cookie-based login. The cookies eliminate additional login prompts when MS-Word opens a document using WebDAV. Typically, the component keeps the dll from doing forms-based logins on Web page because most users do not want this. However, users that do want forms-based logins can get them by following the instructions below.

42.6.2 Solution

An additional configuration change must be made to allow forms-based login with the WebDAV component. To use the WebDAV component with the ExtranetLook component, set `WebDAVDisableOtherFilterCookies=false`.

42.7 Content Item "Stuck" in Auto-Contribution Workflow Step

A content item was dragged and dropped into a folder, and the content item automatically entered a workflow (as expected). However, the content item seems "stuck" in the auto-contribution step of the workflow. The only way to approve the content item is to check it out and check it back in with the **Revision Finished Editing** option selected, so that the content item moves to the first step of the workflow.

42.7.1 Cause

A change was made to the default workflow behavior when content items are contributed through the WebDAV interface. In Folders revision 91 and higher, a content item enters a

workflow in the contribution step when contributed to a folder rather than the first step in the workflow, which used to be the default. This change supports Site Studio's preview modes, so that a content item did not advance into the workflow proper and it could be approved using the Site Studio interface. However, if not using Site Studio, this may not be the anticipated behavior.

42.7.2 Solution

Two configuration entries are available to address this issue:

- `AutoContributorAdvancesOnUnlock`: Enabling this configuration entry makes the content advance immediately to the first workflow step as it did in versions of the Folders component before revision 91.
- `AutoContributorAllowsReview`: This configuration entry enables users to approve a content item in a contribution step of a workflow without having to perform a check-out/check-in sequence.

42.8 Deleting Content from Contribution Folders for Site Studio Website

When documents are deleted from folders used to contribute to a Site Studio website, those documents still appear in dynamic lists on the website.

42.8.1 Cause

If the Trash Bin feature is enabled during the Folders component installation, a Trash Bin is created to contain any content deleted from within folders. A side-effect in Site Studio is that documents deleted from WebDAV folders still appear in Site Studio dynamic lists (such as tables of content) and queries. Explicitly delete the documents from the Trash Bin to make them disappear from all dynamic lists and queries of the Site Studio website.

42.8.2 Solution

To avoid having to delete the documents twice, disable the trash bin. **After you disable the Trash Bin, deleted documents cannot be restored.**

42.9 WebDAV Drag and Drop Does Not Work with Windows 2000

Attempting to drag and drop using any WebDAV client produces no file, or a file containing 0 bytes. Although the action does not successfully complete, no error message is displayed. A copy and paste of the file using the WebDAV client does work.

42.9.1 Cause

The problem is a known issue on some versions of Windows 2000 with Office 2000 Service Release 1 or later which have been upgraded.

42.9.2 Solution

To work around or resolve the drag and drop issue:

- Use copy and paste to add content in situations where the drag and drop does not work.
- Upgrade your Windows dll files as outlined in the following Microsoft knowledge base article at the following URL:

http://support.microsoft.com/default.aspx?scid=kb;en-us;288440

42.10 Folder Shortcuts Do Not Show Latest Changes

If you create a shortcut to a Web folder and use it to open the folder, the folder does not show recent changes to the folder contents.

42.10.1 Cause

Folder shortcuts can show cached information that is no longer current. The problem is a known issue in Microsoft Windows.

42.10.2 Solution

Refresh the folder display by pressing **F5** or choosing **Refresh** from the View menu.

42.11 Profile Rule for All WebDAV Requests

How do I create a profile rule that affects all WebDAV requests?

42.11.1 Solution

Check for the `IsWebdavRequest` variable in your profile rule. For example, you can use the following script for the dOutDate field to verify it is set to 30 days in the future for all WebDAV check ins:

```
<$if IsWebdavRequest$>
<$dprDerivedValue=dateCurrent(30)$>
<$endif$>
```

43
Troubleshooting Inbound Refinery

This chapter describes troubleshooting measures for Inbound Refinery.

The following topics are discussed in this chapter:

- Troubleshooting PDF Conversion Problems
- Troubleshooting Tiff Converter Problems
- Troubleshooting XML Converter Problems

43.1 Troubleshooting PDF Conversion Problems

Inbound Refinery can convert native files to PDF by either exporting to PDF directly using Oracle Outside In PDF Export (included with Inbound Refinery) or by using third-party applications to output the native file to PostScript and then using a third-party PDF distiller engine to convert the PostScript file to PDF. PDF conversions require the following components to be installed and enabled on the Inbound Refinery server:

This section discusses the following topics:

- Troubleshooting Process for PDF Conversion Issues
- Common Conversion Issues
- Inbound Refinery Setup and Run Issues
- PDF Display Issues

43.1.1 Troubleshooting Process for PDF Conversion Issues

The vast majority of PDF conversion issues fall into one of the following categories:

- When a file is checked into the Content Server, a PDF is not generated.
- A PDF is generated, but there are problems with the output.

When troubleshooting PDF conversion issues, you should first try to identify if the issue is related to just one specific file, all files of that type, or all files. For example, if you are having problems converting a Microsoft Excel document to PDF, try checking in other Microsoft Excel documents; preferably files that are smaller and less complex. If the problem is specific to a single file, the problem is most likely related to something within the file itself, such as file corruption, file setup and formatting, and so forth.

If a PDF is not generated when a file is checked into the Content Server, follow basic troubleshooting:

1. Look at the Inbound Refinery and agent logs and identify which step of the conversion process failed (printing to PostScript, PostScript to PDF conversion, etc.). For more information about viewing Inbound Refinery and agent logs and enabling verbose logging for agents, see Configuring Inbound Refinery.
2. If the file is timing out during conversion, first try checking in another, smaller, less complex file of the same type. If multiple files are timing out, adjust your timeout values

and re-submit the files for conversion. For more information about configuring timeout values, see Configuring Inbound Refinery.

3. If the file is failing to print to PostScript, try printing the file to PostScript manually. Most failure to print to PostScript issues are related to the following possible causes:
   - The IDC PDF Converter PostScript printer is not installed.
   - The IDC PDF Converter PostScrpt printer is not named or set up properly.
4. If the file is printing to PostScript successfully but failing to convert to PDF, again first try checking in another, smaller, less complex file of the same type. If the problem is not specific to a single file, or you cannot identify a problem within the files that is causing the conversion to fail, the problem is most likely related to the distiller engine that you are using.

43.1.2 Common Conversion Issues

Content items are often converted incorrectly, or not at all, for the following reasons:

- **Information within the document is outside of the document's print area**: Depending on the native application used to create the document and how your system is set up, a document is sometimes printed to a PostScript file, and the PostScript file is then converted to PDF. Therefore, any information in the document that is outside of the document's print area will not be included in the generated PDF.
- **Inbound Refinery is trying to convert a file that is not appropriate for the conversion engine**: For example, if a file from an application other than Microsoft Word has the extension *doc*, the document is opened in Microsoft Word, which is not correct. The conversion will then fail.
- **The third-party application that is used for conversion starts up with items that require user interaction, such as startup dialogs, tip wizards, or update notices**: This prevents Inbound Refinery from processing and converting the files correctly, and the conversion will time out. Always turn off all such features before using a third-party application for conversion purposes.
- **The Inbound Refinery's Java Virtual Machine (JVM) is frozen:** This is usually associated with failed attempts to convert invalid file formats. Restarting Inbound Refinery will usually fix this problem.
- **Inbound Refinery did not have enough time to process the file**: You can detect this by filtering for the conversion status *PassThru* in Repository Manager. You can also look at the Inbound Refinery and agent log files. Prevent future occurrences of this problem by increasing the appropriate conversion factor on the Timeout Settings page in the Inbound Refinery administration interface.
- **The content item was converted correctly but you cannot view the generated PDF file in Adobe Acrobat or Acrobat Reader.** You might be using an old Acrobat version. In order to ensure that you can view all generated PDF files correctly, you should always use the latest version of Adobe Acrobat or Adobe Acrobat Reader.
- **A Microsoft Office file and a link within that file does not convert correctly.** It is possible that the link is not formatted correctly or is not supported by Inbound Refinery.

43.1.3 Inbound Refinery Setup and Run Issues

The following are symptoms of Inbound Refinery setup and run issues when converting PDF:

- Inbound Refinery Won't Process Any Files
- Missing IDC PDF Converter Printer
- Error: 'Unable to convert. The printer is not installed'
- Error: 'Unable to convert. Not printing to 'c:/temp/idcoutput.ps'.'
- Conversions Keep Timing Out
- Microsoft Word Files Won't Convert
- Microsoft Excel Files Won't Convert
- Microsoft PowerPoint Files Won't Convert
- Microsoft Visio Files Won't Convert
- FrameMaker Files Won't Convert
- WordPerfect Files Won't Convert

43.1.3.1 Inbound Refinery Won't Process Any Files

Inbound Refinery has been installed, but no files are being converted.

Possible Causes	Solutions
File formats and conversion methods not set up for file type in the Content Server.	Use the File Formats Wizard or Configuration Manager in the Content Server to set up the file formats and conversion methods for PDF conversion. For more information, see Configuring Inbound Refinery

43.1.3.2 Missing IDC PDF Converter Printer

The IDC PDF Converter Printer is missing from the list of local printers and documents are stuck in GENWWW. Rebooting the server did not resolve the issue.

Possible Causes	Solutions
The Print Spooler service might not be running.	This service ensures that all installed printers are available, including the IDC PDF Converter printer. Check in the Windows services console (accessible by choosing **Control Panel**, then **Administrative Tools**, then **Services**) to verify this service is running and set to start automatically. If the service is not running, the Inbound Refinery cannot locate and use the IDC PDF Converter printer and documents will be stuck in GENWWW. With the startup type of the Printer Spooler service set to Automatic, this service starts every time the computer boots. After starting the Print Spooler service, you can use Repository Manager to resubmit the documents stuck in GENWWW. Assuming that there are no other conversion issues, the system should now be able to convert documents to PDF successfully.

43.1.3.3 Error: 'Unable to convert. The printer is not installed'

Inbound Refinery is not converting any files to PDF, and the following error message appears in the Inbound Refinery log:

Unable to convert. The printer 'IDC PDF Converter Printer' is not installed.

Possible Causes	Solutions
The IDC PDF Converter printer is not installed.	Install the IDC PDF Converter printer.

43.1.3.3.1 Error: 'Unable to convert. Not printing to 'c:/temp/idcoutput.ps'.'

Inbound Refinery is not converting any files to PDF, and the following error appears in the Inbound Refinery log:

```
Step MSOfficeToPostscript forced conversion failure passthru by conversion engine with error: ''Unable to convert. The printer 'IDC PDF Converter' is not printing to 'c:/temp/idcoutput.ps'.''
```

Possible Causes	Solutions
The IDC PDF Converter printer is not printing to the correct port.	The IDC PDF Converter printer must be set to print to the correct port. The default port is `c:\temp\idcoutput.ps`. The default port can be changed by adding the `PrinterPortPath` variable to the `intradoc.cfg` file located in the refinery *`IntradocDir`*`\bin\` directory and specifying the port path. In this case, the IDC PDF Converter printer should be set to print to the port specified in the `intradoc.cfg` file.

43.1.3.4 Conversions Keep Timing Out

Inbound Refinery conversions keep timing out.

Possible Causes	Solutions
Files are password protected.	Password-protected files will bring up a dialog window during conversion, which will cause the conversion to time out if the dialog is not cleared manually. Remove password protection from files before checking them in.
Your timeout settings are not sufficient.	Adjust your timeout settings. For more information about configuring timeout values, see Configuring Inbound Refinery

43.1.3.5 Microsoft Word Files Won't Convert

Microsoft Word files fail to convert.

Possible Causes	Solutions
Automatic spell checking and grammar checking are causing the conversions to time out.	Turn off the Excel options to perform spell checking and grammar checking automatically.
You are using Word and your security level is too high and is causing the conversions to time out.	Set the Word security level to *low* so Word does not prompt to enable/disable macros when a file with macros is opened.
You are using Word 2003 and the Customer Experience Improvement Program is causing the conversions to time out.	Turn off *Show content and links from Microsoft Online* on the **Tools, Options, General** tab under the Online category, and opt out of the Customer Experience Improvement Program on the **Tools, Options, General** tab under the Customer Feedback category.

43.1.3.6 Microsoft Excel Files Won't Convert

Microsoft Excel files fail to convert.

Possible Causes	Solutions
Automatic calculations are causing the conversions to time out.	Turn off the Excel option to perform calculations automatically.
Automatic spell checking and grammar checking are causing the conversions to time out.	Turn off the Excel options to perform spell checking and grammar checking automatically.
You are using Excel and your security level is too high and is causing the conversions to time out.	Set the Excel security level to *low* so Excel does not prompt to enable/disable macros when a file with macros is opened.
You are using Excel and the Customer Experience Improvement Program is causing the conversions to time out.	Turn off *Show content and links from Microsoft Online* on the **Tools, Options, General** tab under the Online category, and opt out of the Customer Experience Improvement Program on the **Tools, Options, General** tab under the Customer Feedback category.

43.1.3.7 Microsoft PowerPoint Files Won't Convert

Microsoft PowerPoint files fail to convert.

Possible Causes	Solutions
Automatic spell checking and grammar checking are causing the conversions to time out.	Turn off the PowerPoint options to perform spell checking and grammar checking automatically.
You are using PowerPoint and your security level is too high and is causing the conversions to time out.	Set the PowerPoint security level to *low* so PowerPoint does not prompt to enable/disable macros when a file with macros is opened.
You are using PowerPoint and the Customer Experience Improvement Program is causing the conversions to time out.	Turn off *Show content and links from Microsoft Online* on the **Tools, Options, General** tab under the Online category, and opt out of the Customer Experience Improvement Program on the **Tools, Options, General** tab under the Customer Feedback category.

43.1.3.8 Microsoft Visio Files Won't Convert

Microsoft Visio files fail to convert.

Possible Causes	Solutions
You are using Visio and the Customer Experience Improvement Program is causing the conversions to time out.	Turn off *Show content and links from Microsoft Online* on the **Tools, Options, General** tab under the Online category, and opt out of the Customer Experience Improvement Program on the **Tools, Options, General** tab under the Customer Feedback category.

43.1.3.9 FrameMaker Files Won't Convert

FrameMaker files fail to convert.

Possible Causes	Solutions
The files are structured FrameMaker files.	Structured FrameMaker files are most likely fail to convert. A dialog box is displayed when a structured FrameMaker file is opened, which will cause the conversion to time out unless the dialog box is cleared manually.

43.1.3.10 WordPerfect Files Won't Convert

WordPerfect files fail to convert.

Possible Causes	Solutions
The files are old WordPerfect files.	WordPerfect files created in versions prior to version 6 might not be processed effectively. Convert these files to a more recent version of WordPerfect before checking them in.

43.1.4 PDF Display Issues

The following are symptoms of display issues for PDF files generated by Inbound Refinery:

- Blank PDF files in Internet Explorer
- Error: 'File does not begin with '%PDF-'
- PDF Files Don't Open Within Browser Window
- Problems Printing PDFs Using Adobe Acrobat 6.0
- Problem Displaying Internal Thumbnails When Viewing PDF Files

43.1.4.1 Blank PDF files in Internet Explorer

When attempting to open PDF files in Microsoft Internet Explorer, a blank PDF file is displayed.

Possible Causes	Solutions (refer to:)
An old version of Adobe Acrobat Reader is being used that does not support in-place activation.	http://support.microsoft.com/default.aspx?scid=http://support.microsoft.com:80/support/kb/articles/q177/3/21.asp&NoWebContent=1
You have a slow connection, the server has a high load, or the PDF file is very large.	http://support.microsoft.com/default.aspx?scid=http://support.microsoft.com:80/support/kb/articles/q177/3/21.asp&NoWebContent=1
The ActiveX control is corrupt. For Adobe Acrobat Reader 4 to use in place activation with Internet Explorer, the `Pdf.ocx` and `Pdf.tlb` files must be present in the *acrobat_install_dir*`\Program Files\Adobe\Acrobat 4.0\Acrobat\ActiveX` directory.	http://www.adobe.com/support/

43.1.4.2 Error: 'File does not begin with '%PDF-'

When attempting to open a PDF file in a web browser, you receive the following error message:

"...File does not begin with '%PDF-'"

Possible Causes	Solutions (refer to:)
The PDF file has an `.mme` file extension rather than a `.pdf` file extension.	http://www.adobe.com/support/

43.1.4.3 PDF Files Don't Open Within Browser Window

When viewing PDF files generated by Inbound Refinery through a web browser, the PDF files do not open within the browser window.

Possible Causes	Solutions
Settings in Adobe Acrobat Reader or Acrobat.	In Acrobat Reader or Acrobat, verify that Preferences are set for *Web Browser Integration/ Display PDF in Browser*. The exact setting depends of version of Acrobat Reader or Acrobat that you are using.

43.1.4.4 Problems Printing PDFs Using Adobe Acrobat 6.0

When you try to print a PDF, the document will not print and the following message is displayed: *Could not start print job*.

Possible Causes	Solutions
You have Adobe Acrobat 6.0 installed. Adobe Acrobat 6.0 is unable to print a PDF when a file name and URL has more than 256 characters. URLs in workflow and subscription email notifications can easily exceed 256 characters.	Adobe has fixed this problem in Adobe Acrobat 6.0.1. Download and install Adobe Acrobat 6.0.1 or higher to solve this problem.

43.1.4.5 Problem Displaying Internal Thumbnails When Viewing PDF Files

When you view a PDF file, internal thumbnails (thumbnails of the pages within the PDF file) do not display properly. They might display with poor quality, display as grey rectangles, or not display at all.

Possible Causes	Solutions
You are using Adobe Acrobat Reader 5 or 6, and the PDF file is being byte served from the web server. As of Acrobat 5, internal thumbnails can be embedded in the PDF by the creating application, or the viewing application can attempt to create thumbnails dynamically from the rendered pages. If the thumbnail is being generated in Acrobat Reader dynamically, the PDF is being byte served from the web server, and the internal thumbnails are not embedded in the PDF, certain versions of Reader might not be able to render the internal thumbnails properly. This is because the full image data for a given page is on the web server and not available on the client to render the thumbnail image. It is also possible that certain versions of Acrobat Reader might not display internal thumbnails for any PDF that are byte served from the web server.	Possible solutions include: Use Acrobat Reader 7 or higher. This issue appears to be fixed in Acrobat Reader 7. Configure the application that is creating your PDFs (your PostScript to PDF distiller engine or other third-party application) to embed internal thumbnails. Disable byte serving of PDF files on the web server.

43.2 Troubleshooting Tiff Converter Problems

This section discusses the following topics regarding problems encountered during Tiff conversion:

- Installation Problems
- General Conversion Problems
- CVista PdfCompressor Conversion Problems
- PDF Thumbnailing and Viewing Problems

43.2.1 Installation Problems

The following table lists common problems with installing Inbound Refinery, possible causes, and solutions.

Problem	Possible Causes	Solutions
Refinery or Content Server would not start after Tiff Converter components are installed	Wrong component installed on content server/refinery.	Uninstall the components and reinstall the components on the correct location.

43.2.2 General Conversion Problems

The following table lists general Inbound Refinery conversion problems, possible causes, and solutions.

Problem	Possible Causes	Solutions
TIFF files are not being converted (they are being passed through in their native format).	File formats and conversion methods for Inbound Refinery have not been set up properly in Content Server.	Set up file formats and conversion methods for Inbound Refinery. For details, see Managing Tiff Conversions.
TIFF files are not being converted (they are being passed through in their native format).	The conversions are taking too long, and Inbound Refinery is timing out.	Change your Inbound Refinery timeout settings. For details, see Changing Timeout Settings .
TIFF files are not being converted (they are being passed through in their native format).	Inbound Refinery is failing to launch CVista PdfCompressor.	Ensure that the PdfCompressor path is correct. For details, see Configuring CVista PdfCompressor OCR Languages.
Zipped TIFF files are not being processed by Inbound Refinery when they are checked in.	File formats and conversion methods for Inbound Refinery have not been set up properly in Content Server.	Change how zip files are processed. For details, see Changing Timeout Settings .
The TIFF Conversion conversion method is not available in the Content Server Configuration Manager.	The TiffConverterSupport component has not been uploaded and enabled.	Upload and enable the TiffConverterSupport component using either the Component Wizard or the Component Manager. This component is included on the Inbound Refinery distribution media.
The TIFF Conversion conversion method is not available in the Content Server Configuration Manager.	The TiffConverterSupport component is enabled, but Content Server has not been restarted.	Restart Content Server.

43.2.3 CVista PdfCompressor Conversion Problems

The following table lists common conversion problems when using CVISION CVista PdfCompressor, possible causes, and solutions.

Problem	Possible Causes	Solutions
Inbound Refinery is failing to launch CVista PdfCompressor.	The path to the *CVista PdfCompress.exe* is incorrect.	Ensure that the PdfCompressor path is correct. For details, see Configuring CVista PdfCompressor OCR Languages.

Problem	Possible Causes	Solutions
I have used the CVista PdfCompressor user interface to change conversion settings, but this has had no effect on how TIFF files are being processed.	Changes made in the CVista PdfCompressor user interface will not affect how CVista PdfCompressor functions when called by Inbound Refinery.	Change the CVista PdfCompressor configuration settings using the Inbound Refinery user interface. For details, see Configuring CVista PdfCompressor OCR Languages.
CVista PdfCompressor is only performing OCR on English text.	By default, CVista PdfCompressor uses only an English OCR dictionary. Other OCR languages must be set up.	Set up multiple OCR languages for CVista PdfCompressor. For details, see Configuring CVista PdfCompressor OCR Languages.

43.2.4 PDF Thumbnailing and Viewing Problems

The following table lists common problems with creating thumbnails for and viewing the PDF files that are generated by Inbound Refinery, possible causes, and solutions.

Problem	Possible Causes	Solutions
No thumbnails are being created for PDF files generated by Inbound Refinery.	Thumbnailing is not enabled in Inbound Refinery.	Enable thumbnailing in Inbound Refinery.
When viewing PDF files generated by Inbound Refinery in Adobe Acrobat Reader, there are lines or other artifacts on the screen.	Acrobat Reader 4 is being used to view the files.	When viewing PDF files generated by Inbound Refinery, use Adobe Acrobat Reader 6.0.1 or higher for the best results.

43.3 Troubleshooting XML Converter Problems

Two areas have been identified as possible problems when converting XML.

After installing Inbound Refinery, a Content Server or refinery instance will not start or is not functioning properly.

Possible Causes	Solutions
The XMLConverter component has been installed on a Content Server, or the XMLConverterSupport component has been installed on a refinery.	The XMLConverter component must be installed on refineries, and the XMLConverterSupport component must be installed on Content Servers. If you install the wrong component, complete the following: • Uninstall the component from the Content Server or refinery using the Component Manager or the Component Wizard. • Install and enable the correct component.

XML Converter has been installed, but no files are being converted.

Possible Causes	Solutions
File formats and conversion methods not set up for file type in the Content Server.	Use the File Formats Wizard or Configuration Manager in the Content Server to set up the file formats and conversion methods for XML conversion. For details, see Configuring Content Servers to Send Jobs to Refineries.
The refinery has not been configured to accept the conversion.	Configure the refinery to accept the conversion. For details, see Setting Accepted Conversions.
The refinery has not been configured to create XML files as the primary web-viewable rendition or an additional rendition.	For details, see Setting XML Files as the Primary Web-Viewable Rendition and Setting XML Files as an Additional Rendition.