Oracle® Universal Records Management

Records Manager DoD Edition System Setup Guide

10g Release 3 (10.1.3.3.0)

April 2007

Records Manager DoD Edition System Setup Guide, 10g Release 3 (10.1.3.3.0)

Contributing Authors: Ron van de Crommert, Jean Wilson

Contributors: Lisa Jones, Tok Hui Mackenthun, Victor Owuor

Table of Contents

Chapter 1: Introduction

Chapter 2: Introduction to Records Management

Chapter 3: Quick Start Setup

Chapter 4: DoD Edition Interface

Chapter 5: Setting Up Security

Chapter 6: Additional Security Settings

Chapter 7: General Configuration Options

Chapter 8: Setting Up a Retention Schedule

Chapter 9: Setting up Triggers

Chapter 10: Configuring Time Periods

Chapter 11: Custom Metadata Fields

Chapter 12: Configuring Dispositions and Freezes

Chapter 13: Configuring Related Content (Links)

Chapter 14: Defining Disposition Instructions

Chapter 15: Using Profiles

Appendix A: Third Party Licenses

Chapter

1

INTRODUCTION

OVERVIEW

This section covers the following topics:

- About This Guide (page 1-1)
- What's New (page 1-3)
- Documentation and Help (page 1-3)

ABOUT THIS GUIDE

Note: This system administration guide assumes you are using the Trays layout.

This guide provides instructions to set up and administer the Records Manager DoD Edition software on the content server. The information contained in this document is subject to change as the product technology evolves and as hardware, operating systems, and third-party software are created and modified.

Symbols

The following symbols are used throughout this document:

Symbol	Description
💡	**Note:** Brings special attention to information.
⚙	**Tech Tip:** Identifies information that can be used to make your tasks easier.
❗	**Important:** Identifies a required step or required information.
✖	**Caution:** Identifies information that might cause loss of data or serious system problems.
🔑	**Permissions:** Indicates what specific permissions are needed to perform tasks.

Conventions

The following conventions are used throughout this document:

- The notation <*Install_Dir*> is used to refer to the location on your system where a specific instance of Content Server is installed.
- Forward slashes (/) are used to separate parts of an Internet address. For example, http://www.microsoft.com/windows2000/. A forward slash might or might not appear at the end of an Internet address. Forward slashes (/) are also used to separate the directory levels in a path name whether on a UNIX or a Windows system. A forward slash always appears after the end of a directory name.
- Paths to access operating system screens use the following formatting structure:

  Start—Settings—Control Panel
- Required user input is distinguished using the following font formatting:
  `xyz_name`

Audience

This guide provides instructions to configure and administer the DoD Edition product. The guide is intended mainly for administrators, records managers, and privileged users responsible for processing records and managing retention policies.

What's New

Several interface changes have been made from Version 7.1.4:

- Retention tasks to be processed are now available on pull-down menus instead of from the Trays menu.
- Advanced screening is no longer available. That functionality has been merged into the regular screening functionality.
- Dormant global triggers as a trigger type are no longer selectable as an option. You can create dormant global triggers by simply not adding an activiation date when you create the trigger.
- The Configure Retention Components page is no longer used to configure aspects of the retention schedule (triggers, dispositions, and so on). All functionality of that type is now available by using pull-down menus which are available throughout the product.
- You can now edit pre-defined link (related content) types. By default the main links with new content item revisions is checked. This can be changed so linking is not revision independent.

Installation Notes

Case-insensitive searches are not peformed by default when using the DoD Edition product for database searches (for example, in screening, audits, reviews or disposition listings). If you want to perform case-insensitive searches, the databased used must be configured to do so.

Indexing fails for PDF files generated with Inbound Refinery versions prior to 7.6.1 and PDF Converter prior to version 7.6.1.

Documentation and Help

This section covers the following topics:

- Documentation (page 1-4)
- Tooltips (page 1-4)
- Quick Help (page 1-5)

- Help Menu (page 1-5)

Documentation

The following Records Manager DoD Edition documentation is available:

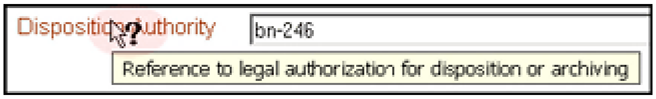
- *Records Manager DoD Edition Installation Guide*
  This document provides information about installing the DoD Edition software on the content server. It is provided as a PDF file on the DoD Edition software distribution media.
- *Records Manager DoD Edition System Setup Guide* (this guide)
  This document provides information about setting up and administering the DoD Edition application on the content server. It is provided as a PDF file and HTML help system, both of which can be accessed from the DoD Edition user interface. The PDF file is also available on the DoD Edition software distribution media.
- *Records Manager DoD Edition System Maintenance Guide*
  This document provides information about administering the DoD Edition application on the content server. It is provided as a PDF file and HTML help system, both of which can be accessed from the DoD Edition user interface. The PDF file is also available on the DoD Edition software distribution media.
- *Records Manager DoD Edition User Guide*
  This document provides information about using the DoD Edition application on the content server. It is provided as a PDF file and HTML help system, both of which can be accessed from the DoD Edition user interface. The PDF file is also available on the DoD Edition software distribution media.

In addition to these guides, you can also access information about the product with context-sensitive tooltips, quick help, and help menu.

Tooltips

If you hover the mouse cursor over a field label in your web browser, you can get context-sensitive information on the field label. A question mark is displayed, and then the tooltip appears.

Figure 1-1 Field label tooltip

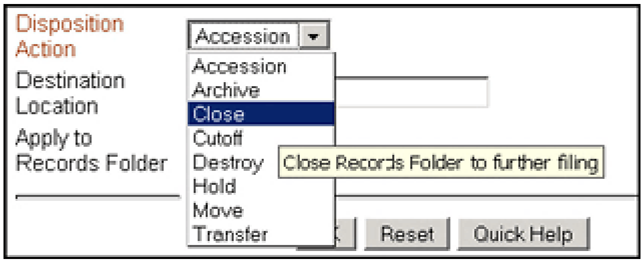


Disposition Authority bn-246

Reference to legal authorization for disposition or archiving

If you are using Netscape or Mozilla as your web browser, you can view tooltips for items in options lists as well, provided the list items are not custom entries.

Figure 1-2 Option list item tooltip (only supported by Netscape and Mozilla browsers)



Quick Help

Click the **Quick Help** button where available on pages and screens to view context-sensitive help for that page or screen.

Help Menu

You can click the main menu Help link to open the online HTML help system for Universal Content Management, which includes the DoD Edition help files. If you are logged in with user privileges, you will only see the end-user help system. If you are logged in as an administrator, you will see the full administrator help system (including the user documentation).

Chapter

2

Introduction to Records Management

Overview

This section covers the following topics:

- Management of Records and Other Retained Items (page 2-1)
- About DoD Edition (page 2-8)
- Basic Retention Management Concepts (page 2-9)
- DoD Edition and Content Server (page 2-12)
- Basic Processes (page 2-13)

Management of Records and Other Retained Items

DoD Edition effectively manages both record and non-record content items on a retention schedule. The focus of Records Management tends to be the ***preservation of records*** for historical or archival purposes while also performing retention management functions. The focus of retention management of non-record content items tends to be the ***scheduled elimination of content*** in which the costs of retaining content outweighs the value of keeping it.

This section covers the following topics:

Needs for Records Management

There are various reasons why organizations may need records management:

- ❖ Regulatory Needs (page 2-2)
- ❖ Litigation Needs (page 2-2)
- ❖ Business Needs (page 2-3)

Regulatory Needs

Many organizations are subject to regulations that require the retention of information for a specified period of time:

- ❖ 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/healthcare industry—HIPAA, FDA regulations
- ❖ Financial services—SEC Rule 17a
- ❖ Telecommunications industry—47 CFR 42, etc.

Records management enables organizations to comply with the retention requirements of these regulations.

Litigation Needs

There may be litigation-related needs for effective and efficient records management:

- ❖ Policy-based retention of records:
  - Retain information that you may need for litigation (for example, a contract and any communication relating to it).

  - Centralized searching and retrieval of that information
- ❖ Systematic disposition of eligible records or non-record content:
  - Less material to search through during discovery
  - Less material to give to opposing counsel
- ❖ Suspend/freeze disposition of records or non-record content items relating to pending litigation:
  - Avoid appearance of cover-up and possible liability when records or non-record content items relating to pending litigation are destroyed.

Business Needs

There may be business-related needs for effective and efficient records management:

- ❖ “Islands of content” problem. Content items that are:
  - Generated across the organization
  - Created in a variety of forms—for example, e-mail, office application documents, sheets of paper, CDs, DVDs, microfiche, recordings of corporate events and conference calls, etc.
  - Stored in an ad-hoc fashion in a variety of locations—for example, employee desks, employee computers, corporate servers, central file storage, offsite storage.
- ❖ There is a need to:
  - Provide a uniform infrastructure for retrieving and sharing the content across the organization.
  - Ensure that content items are retained over the period of time that they are useful to the business.

DoD Edition manages all records and non-record content items, regardless of their source, in a single, consistent, manageable infrastructure.

What Do I Retain?

Both record and non-record content items for retention are any form of information, both physical and electronic that is **important** enough for an organization that it must be **retained** for a specific period and may be **disposed** of when it is no longer needed.

- ❖ DoD 5015 record: As defined above with the stipulation that it is also made or received by an agency of the United States Government. The U.S. Government defines records as follows:

“Records include all books, papers, maps, photographs, machine-readable materials, or other documentary materials, regardless of physical form or characteristics, made or received by an Agency of the United States Government under Federal law or in connection with the transaction of public business and preserved or appropriate for preservation by that agency or its legitimate successor as evidence of the organization, functions, policies, decisions, procedures, operations, or other activities of the Government or because of the informational value in them.”

- Business record: As defined above with the stipulation that it is used in the transaction of public business.
- Non-record content items: As defined above with no additional governmental or public business criteria. However, it can be revisioned, retained (but not necessarily with a minimum retention period), and can be on a disposition schedule.

  Your organization may choose to manage non-record content with DoD Edition to eliminate outdated and misleading information, track documents related to legal proceedings, and manage storage resources. Basically, managing non-records content provides a much simpler deployment of DoD Edition for organizations that do not need a full compliance with DoD5015.

See the following sections for more information:

- Importance of Content (page 2-5)
- Retention (page 2-6)
- Disposal (page 2-6)

How do Records and Non-Record Content Differ?

There are a number of basic differences between records and non-record content retention qualities:

- **Purpose:** Records are essentially historical artifacts, whereas non-record content items for retention are generally live, active documents that can be revisioned.
- **Benefits:** Benefits of managing records is compliance with regulations and corporate retention policies. Benefits of managing non-record content items is reduced risk and cost of discovery for litigation, reduced costs associated with storage, elimination of clutter to promote user efficiency, and dissemination of only current information to improve communication.
- **Ability to Revision:** Records cannot be changed once checked in, which means they cannot be revisioned after they become records. Non-record content items can be checked out, modified, and checked back in to create multiple revisions.

- **Actions Available after Cutoff**:
  - Records can have their metadata edited until they are cut off (when the record status changes and it goes to disposition). Non-record content can have their metadata edited after cutoff.
  - Records that are cut off or frozen cannot be deleted. Non-record content that is cut off can be deleted.
- **Disposition**: Records have disposition schedules assigned by their location in the Retention Schedule. This defines how they should be retained and disposed of, whereas non-record content items generally have disposition schedules (life cycles) assigned by item upon check in.

Note: DoD Edition supports disposition schedules for non-record content items, which means it can manage retention and disposal of non-record content. This enables you to schedule lifecycles for content to eliminate outdated or superseded information, manage storage resources, or handle legal procedures.

- **Filing**: Records can be filed into folders, and non-records can be filed only into categories set up for non-record content. Therefore, documentation about folders and interactions with folders are intended for record-centric content only.
- **Functionality Specific to Records Only**:
  - Classification/Supplemental Markings
  - Permanence
  - Record Folders
- **Functionality Available to Content outside of Retention Schedule**:
  - Freeze
  - Link
  - Subject to Review

Importance of Content

Retained information can be **important** for a variety of reasons:

- The information may be required for the day-to-day operations of the organization and needs to 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 that require the information to be retained (for example, transaction documents, financial statements, lease agreements).
- The data may be important in preparation for possible litigation or discovery.

Retention

The information may need to be **retained** 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 retention may be time-based (for example, five years from the record filing date).
- The retention period may be event-based (for example, an employee termination).
- The retention period may be both time-based and event-based (for example, two years after employee termination).
- The retention may be based on revision (for non-record content items).

Disposal

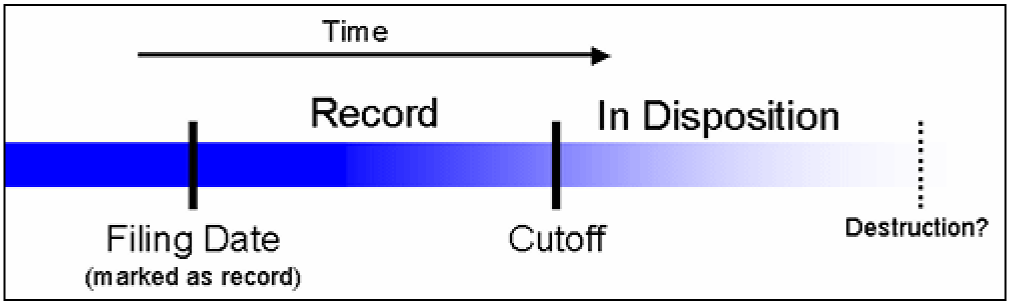
After a retention period, records and non-record content items are disposed of by authorized people according to the requirements of the organization. Disposition actions include:

- Destroy (physical or electronic), possibly after a certain period of retention.
- Store within the organization (physical or electronic).
- Transfer to an external storage facility (physical or electronic).
- Some records are deemed so important that they will never be destroyed (for example, due to their historical significance). Their “disposal” simply means that their status changes from active use or immediate relevance to historical preservation.

Lifecycle for Records

The lifecycle of a record goes through a number of stages.

Figure 2-1 Record life cycle



The **filing date** of a record is the date that a content item becomes a record. This often coincides with the check-in date because most records are checked into the content server as records. However, it is possible for an active content item that is already checked in to be marked as a record.

The **cutoff** of a record or non-record content item is the moment that the status of the item changes and the item goes into disposition. An item may be cut off after a specific period of time, at a specific event, or after a period of time after an event.

Types of Retained Content

Retained content can be divided into categories depending on the perspective:

- Internal and External Retained Content (page 2-7)
- Classified, Unclassified, Declassified Records (page 2-8)
- Non-Permanent, Permanent, Retained Content (page 2-8)

Internal and External Retained Content

An ***internal*** retained content item is an electronic item stored within Content Server and managed by DoD Edition. 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. DoD Edition can then be used to manage the disposition schedule, search metadata associated with the external file, and even manage an electronic rendition of an external file. An electronic rendition can either be checked in as a primary file of an external record, or be filed as a separate file, and then linked to the external file metadata.

Classified, Unclassified, Declassified Records

Records (not non-record content) can be ***classified***, ***unclassified***, or ***declassified***.

Classified records are records that require protection against unauthorized disclosure (for example, because they contain information sensitive to the national security of the United States). Unclassified records are records that are not and have never been classified. Declassified records are records that were formerly classified, but whose classified status has been lifted.

A *classification* specifies the security level of a classified record. A *classification guide* provides default classification values for record check-in pages.

Note: DoD Edition has been certified by the Joint Interoperability Test Command (JITC) to comply with the DoD 5015.2 standard (including Chapter 4). A copy of the standard is available on the official web site 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.

Non-Permanent, Permanent, Retained Content

For disposition purposes, records and non-record content items are categorized into ***non-permanent, permanent***, and ***subject to review***. Most records and non-record content items fall into the non-permanent category. Non-permanent items are usually destroyed after a retention period. Permanent records are deemed important for continued preservation and are retained indefinitely (for example, because of their historical significance). Permanency does not apply to non-record content.

Records and non-records content items can be scheduled for periodic reviews. This can be used for DoD Vital Review of records.

About DoD Edition

DoD Edition enables you to manage records and non-record content items—regardless of their source or format—in a single, consistent, manageable infrastructure. Records and non-record content items managed by DoD Edition are assigned retention schedules and disposition rules. This enables you to schedule lifecycles for content to eliminate outdated or superseded information, manage storage resources, or comply with legal audit holds.

The items and their associated metadata are stored in retention schedules, which are hierarchies with categories that define disposition instructions for records and non-record content. 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 your organization.

DoD Edition is compliant with the DoD 5015.2 standard (including Chapter 4), and certified by the Joint Interoperability Test Command (JITC). 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/.

In addition to records, DoD Edition can also manage disposition schedules of non-record content in the content server. This enables you to schedule lifecycles for content to eliminate outdated or superseded information, manage storage resources, or comply with legal audit holds.

Basic Retention Management Concepts

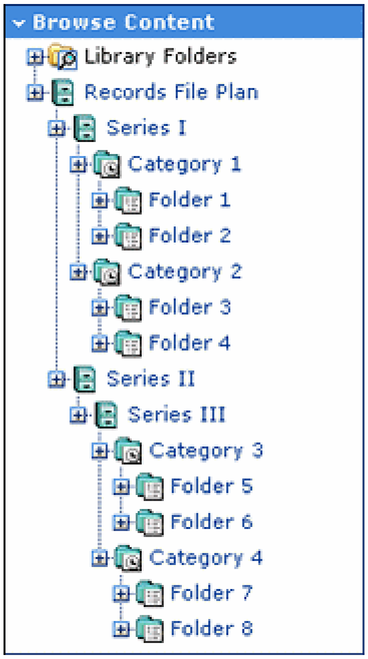
The following concepts are important in the context of DoD Edition:

- Retention Schedules (page 2-10)
- Series (page 2-10)
- Retention Category (page 2-10)
- Records Folder (page 2-11)
- Disposition (page 2-11)
- Disposition Instruction (page 2-11)
- Period (page 2-11)
- Trigger (page 2-11)
- Record or Non-Record Content Item Link (page 2-11)
- Classification (page 2-12)
- Classification Guide (page 2-12)
- Supplemental Marking (page 2-12)
- Freeze (page 2-12)

Retention Schedules

The retention schedule is an organized hierarchy of series, categories, and folders, which enables you to cluster records and non-record content into similar groups, each with its own retention and disposition characteristics (see the figure below).

Figure 2-2 Retention Schedule



Series

A series is an organizational construct in the retention schedule which enables you to organize categories into functional groups. This is especially useful if you have a multitude of categories. Series cannot contain records or non-record content items. A series can be nested, which means a series may contain other series.

Retention Category

A retention category is a set of security settings and disposition instructions in the retention schedule hierarchy, below a series. This enables you to organize records folders, records, and non-record content into groups with the same retention and disposition characteristics. A retention category may contain one or more records folders, records, or non-record 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.

Records Folder

A records folder is a collection of similar records in the retention schedule. This enables records to be organized into groups. A records folder typically follows the security settings and disposition rules associated with its assigned retention category. Records folders can be nested, which means a records folder may contain other records folders. Records folders cannot contain non-record content.

Disposition

Disposition is the collective set of actions taken on records or non-record content items, usually for items that are no longer required. Disposition actions include wait times and activities such as transfer to external storage facilities, the destruction of temporary records or non-record content items, and the replacement of records or non-record content that is subject to review with updated information.

Disposition Instruction

A disposition instruction is created within a retention category, and typically consists of one or more disposition rules, which define how records or non-record content items are handled and what actions should be taken on them (for example, when and how they should be disposed of).

Period

A period is the segment of time that must pass before a review or disposition action can be performed. DoD Edition comes with a number of built-in periods (for example, “one year”), but you can create custom periods to meet your unique business needs.

Trigger

A trigger is an event that needs to take place before a disposition instruction is processed. Triggers are associated with disposition rules for retention categories. Examples of triggering events include changes in status, completed processing of a preceding disposition action, and retention period cutoff.

Record or Non-Record Content Item Link

A record or non-record content item link is a defined relationship between records or non-record content items. This may be useful when items are related and need to be processed together. Links are available for content items that are stored both in and out of the retention schedule.

Classification

A classification specifies the security level of a classified record. It is used in the process of identifying and safeguarding records that contain sensitive information. Typical classification levels are “Top Secret,”, “Secret,” and “Confidential,” and “Unclassified.” Classification is not available for non-record content items.

Classification Guide

A classification guide is a mechanism used to define default values for a number of classification-related metadata fields on the content check-in pages for records (not non-record content). This enables convenient implementation of multiple classification schemes in DoD Edition.

Supplemental Marking

Supplemental markings are extra attributes associated with a record (not non-record content). They can be used to clarify document handling in addition to standard document classifications, and also as a security feature to further restrict users from accessing records folders and records. Supplemental markings can be set at both the records folder and record level.

Freeze

Freezing a records folder, record, or non-record content item inhibits disposition processing for that item or the records in that folder. Frozen records or non-record content items cannot be altered in any way nor can they be deleted or destroyed. This may be necessary in order to comply with legal or audit requirements (for example, as a result of litigation). Freezing is available for records and non-record content items that are stored both in and out of the retention schedule.

DoD Edition and Content Server

DoD Edition supports the following Content Server layouts and search templates (which users can set in their user profile):

- Supported layouts:

- Trays
- Top Menus

❖ Supported search templates:

- Headline View
- Thumbnail View
- My Headline View

Note: The DoD Edition application does not support the Classic layout or the Classic View search template. This guide assumes you are using the Trays layout.

BASIC PROCESSES

The following steps outline the basic workflow of records and non-record content within DoD Edition:

1. The retention schedule and any required components (such as triggers, periods, classifications, and custom security or metadata fields) are created.
2. Records and non-record content 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 by DoD Edition 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 records or non-record content 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 My Retention Assignments links within the DoD Edition 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 in the pending events pages. This is a manual process.

Many disposition schedules are **time-based** according to a predictable schedule. Typically, records are filed and then destroyed a certain number of years later. The system keeps track of when the affected records or non-record content items are due for action. Notification e-mail is sent, and the records folders, records, and non-record content items are routed to the My Retention Assignments area of DoD Edition.

The person responsible for the pending events and reviews then processes the record folders, records, or non-record content items accordingly. The particular disposition actions due are indicated for the record folders, records, or non-record content items. Available menu actions are context-sensitive according to the state of the item. For example, a records folder due for its final disposition step of destruction would have the Destroy commands available, but not the Archive commands.

In contrast, **time-event** and **event-based** dispositions must be triggered with a non-system-derived trigger; that is, a trigger that was defined for a particular scenario. When a pending legal case starts litigation, the records administrator must enable the custom trigger and set its activation date since the start date information is external to the DoD Edition logic. Custom triggers enable you to define event and time-event based disposition actions based on the occurrence of a particular event.

Chapter

3

QUICK START SETUP

OVERVIEW

This chapter provides a broad overview of the tasks needed to set up your DoD Edition system. Use the information in this chapter as a reference to tasks that need to be done. For detailed conceptual and reference information pertaining to these tasks, see the other chapters in this guide.

Caution: If you are unclear about any of the tasks in this chapter, consult the detailed task information in the later chapters in this guide.

Before setting up your system, see Chapter 2 (*Introduction to Records Management)* which provides an essential overview to the concepts and vocabulary used in a record management system.

This chapter covers the following topics:

Permissions: Specific permissions are required to perform the tasks described here. For details about the required permissions, see the tasks outlined in later chapters of this manual. In general, users with the **rmaadmin** role should be able to perform the majority of these tasks.

SETUP CHECKLIST

The following checklist provides an overview of the steps needed to set up DoD Edition. 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.

This checklist spans multiple sections of this guide. With the table of contents and index, this checklist also serves as a documentation road map for finding the information you need.

Tech Tip: To record everything you are doing while setting up and configuring DoD Edition, you may want to configure the audit trail first. See the *Records Manager DoD Edition System Maintenance Guide* for details. All user actions are set to be recorded by default.

Setup tasks include the following topics. Note that some of these tasks may be optional depending on your organization. For example, you may not need to configure your root nodes or add custom metadata. The information is provided so you can determine if the step may be useful or not.

- ☐ Configure security. See Security Overview (page 3-4) for an overview and Chapter 5 *(Setting Up Security)* for details.
- ☐ Determine additional security settings. See Classification Security Settings (page 3-6) for an overview and Chapter 6 *(Additional Security Settings)* for details.
- ☐ Configure system settings. See System-Wide Configuration (page 3-9) for an overview and the following sections for details:
  - Setting the Fiscal Calendar (page 7-10) for financial and accounting purposes.
  - Setting the Default Notification Recipient(s) (page 7-11) for e-mail notifications.
  - Managing Time Periods (page 10-2), used to define the time associated with retention or disposition of records.
  - Managing Custom Metadata (page 11-2) required for your organization.

- ❑ Set up the retention schedule. See Setting Up a Retention Schedule (page 3-11) for an overview and the following sections for details about configuring the organization of records. This includes:
  - Configuring the Root Nodes (page 7-12), allowing you to hide retention schedules, view root node information or generate reports.
  - Managing Series (page 8-15), used to manage the view of different retention schedule hierarchies.
  - Managing Retention Categories (page 8-22), which define security settings and disposition instructions for that category.
  - Managing Records Folders (page 8-31) used in the retention schedule.
- ❑ Determine how records will be handled. See Configuring Content Triggers, Dispositions, and Freezes (page 3-13) for an overview and the following chapters for details:
  - Managing Triggers (page 9-6). Triggers are used to initiate events that affect records.
  - Custom Disposition Actions (page 12-3), which define the sequence of actions to be performed on records during their life cycle.
  - Managing Freezes (page 12-14) to inhibit disposition processing.
  - Managing Dispositions (page 12-3) for retention categories and records folders.
- ❑ Establish relationships between content. Use Managing Related Content (page 13-9) to establish a type of relationship between individual records and content items. See Chapter 13 (*Configuring Related Content (Links)*) for complete details.

Additional tasks discussed in the *Records Manager DoD Edition System Maintenance Guide* include importing and exporting archives and configuring the audit trail, which tracks activities.

After configuring DoD Edition, users with the appropriate rights can file, search, and link records and content and generate retention schedule reports. For more information, see the *Records Manager DoD Edition User Guide.*

The core processing performed by records administrators during the use and maintenance phases of the records life cycle, such as screening and cycling records and content, is discussed in the *Records Manager DoD Edition System Maintenance Guide*.

Security Overview

Multiple layers of security are available in DoD Edition. Permissions and privileges are determined by the intersection of all security mechanisms in place. The strictest setting prevails. See Chapter 5 (*Setting Up Security)* for complete details.

This section discusses the following topics:

- ❖ Security in DoD Edition (page 3-4)
- ❖ Setting Security Preferences (page 3-5)
- ❖ Rights for Roles (page 3-6)
- ❖ Classification Security Settings (page 3-6)

Security in DoD Edition

The following security elements are used to define user roles and permissions:

- ❖ ***Predefined user roles***, discussed in detail in Roles (page 5-3). Each of these predefined roles comes with a default set of permissions and rights, but these can be modified to suit your specific needs. These include the following roles:
  - **rma,** generally assigned to basic records users. It allows them to perform basic records management tasks.
  - **rmaprivileged**, generally assigned to basic records users who need additional privileges (for example, creating triggers or folders, and modifying record attributes).
  - **rmaadmin,** generally assigned to administrators who set up and maintain the infrastructure and environment.
- ❖ ***Rights*** control access to functions assigned to Content Server 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. See Assigning Rights to User Roles (page 5-19) for details.
- ❖ ***Security groups*** define security on a group of content. Records Manager DoD Edition comes with a predefined security group called “RecordsGroup.” Users with the predefined ‘rma’ or ‘rmaprivileged’ roles have read and write permission (RW) to the RecordsGroup security group. Users with the ‘rmaadmin’ role have read, write, delete, and admin permission (RWDA) to this security group. For details, see Security Groups (page 5-16).

- ***Access control lists*** (ACLs) manage the security model on dispositions. You can assign ACLs to records folders, triggers, and retention categories. ACLs are used to control user and group access permissions for triggers, categories, and records folders. You can assign the ACL for each category, records folder, and trigger you create. See Access Control Lists (ACLs) (page 5-16) for details.

Setting Security Preferences

Security preferences are set on the Configure Records Management Page (page 7-2). The security preferences set on that page are in addition to those provided with Content Server.

Caution: After your production environment is underway, we recommend you do not change the security settings for ACLs or the default Content Server security. Doing so can cause unforeseen consequences.

To configure security settings, log in as an administrator and select **Configure Records Management** from the **Administration** tray. Select the options you want to use:

- To use Access Control List Security, select the **ACL-based security** check box.
- To activate the default security in Universal Content Management, select the **Default Content Server security on Categories, Folders, and Triggers** check box. To not set the additional security on categories, records folders, and triggers, clear the check box.
- (Required for DOD 5015.2 compliance): To use supplemental markings, select the **Supplemental Marking** check box. For more information, see Supplemental Markings Details (page 6-3). To make users match all supplemental markings, select the **User must match all Supplemental Markings** check box. To allow a user to match only one supplemental marking, clear the check box.
- To create your own custom security fields, select the **Custom Security Fields** check box.
- To use classified record security, select the **Classified Security** check box. For more information, see About Records Classification (page 6-14).

When done, click **Submit Update**.

Rights for Roles

Rights define what actions users can perform on record or non-record content items. To assign rights to user roles, select **Admin Applets** from the **Administration** tray.

Click the **User Admin** icon and choose **Security—Permissions by Role** from the menu. Select the role to review or modify. Click **Edit RMA Rights** then set the appropriate rights by selecting or clearing the check boxes on the various tabs. Click **OK** when you finish.

See Assigning Rights to User Roles (page 5-19) for details.

Classification Security Settings

Supplemental markings, classifications, and classification guides can be used to provide further security for your environment and to organize classified documents.

See Chapter 6 (*Additional Security Settings)* for complete details about additional security settings. This section covers the following topics:

- Supplemental Markings (page 3-6)
- Security Classifications (page 3-7)
- Classification Guides (page 3-8)

Supplemental Markings

Note: To disable use of supplemental markings as a security feature, clear the *Supplemental Markings* check box on the Configure Records Management Page (page 7-2) and do not assign the markings to users.

When you assign supplemental markings to users, even if a user has access to a specific records folder, the supplemental marking further restricts access to folders and records. In circumstances where a folder or record has multiple supplemental markings, you can require that a user match all assigned supplemental markings to access a record or records folder. Otherwise (that is, when ‘match all’ is disabled), if a user matches just one of the multiple supplemental markings, the user can access the record or records folder object.

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

You can enable and disable supplemental markings at any time. To enable or disable markings, select or clear the **Supplemental Markings** check box on the Configure Records Management Page (page 7-2).

To create a supplemental marking, click **Add** in the Supplemental Marking area of the Configure Records Management Page (page 7-2). Enter a name and a description then click **Create**.

To assign a marking to a user, select **Admin Applets** from the **Administration** tray. Click the **User Admin** icon. On the Users tab, select the user in the Users list, and click **Edit**. In the **Supplemental Markings** field, select the markings to which the user should have access. Click the options list arrow, and click the marking you want. You can assign multiple markings to a user. Click **OK** and repeat the process for each user you need to assign supplemental marking access. Restart the content server when done.

Security Classifications

Records classification can be an additional way to restrict records access in conjunction with supplemental markings and custom security fields. Classification markings are at the record level only, unlike supplemental markings, which are at the record **or** record folder level.

A number of classification features are available that are used to handle and process classified records in accordance with the Chapter 4 requirements of the DoD 5015.2 specification. Several built-in records classifications (“Top Secret,” “Secret,” and “Confidential”) are available, but you can also create your own custom classifications (see Creating or Editing a Security Classification (page 6-18)).

Records are either classified, unclassified, or declassified. **Classified records** have an initial classification and a current classification. **Unclassified records** are any records that are not and have never been classified. **Declassified records** are any records that were 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, you can enable and disable classified security at any time. After enabling, you can create custom security classifications. If you create any additional security classifications, make sure you indicate its place within the marking hierarchy. For further information, see Setting the Order of Security Classifications (page 6-19).

To enable security, click the **Classified Security** check box on the Configure Records Management Page (page 7-2). Click **Submit**. To disable classified security, clear the **Classified Security** check box.

Caution: Disabling classified security puts sensitive classified records at risk of being accessed by unauthorized people. After your classified security is in force, it is not recommended that you disable it.

To create a new security classification, select **Configure—Security Classification** from the Configure Records Management Page (page 7-2). Click **Add** on the Configure Security Classification Page (page 6-24). Enter a unique classification name and description. Click **Create** then click **OK**. To view the classification, you must have this classification level or a higher level assigned to your login ID. You must also indicate the placement of the new classification in the hierarchy.

Use the up or down arrow on the Configure Security Classification Page (page 6-24)to move the selected security classification to a new place in the classification hierarchy. The highest classification should be at the top of the list, and the lowest at the bottom. Click **Submit Update** when done.

For further details, see Setting the Order of Security Classifications (page 6-19).

Important: The last item in the list will be unclassified regardless of the name that you assign to it. Make sure that you have a “classification” in your hierarchy that you intend to be unclassified.

To assign security classifications to users select **Admin Applets** from the **Administration** tray. Click the **User Admin** icon. On the Users tab, select the user in the Users list, and click **Edit**. The Edit User screen is displayed.

Make sure the Info tab is active. In the **Security Classification** field, select the maximum security level that the user should have access to from the option list available on the pull-down menu. Click **OK**. Repeat the process for each user.

Classification Guides

Note: Classification guides are for record content only. They cannot be used with non-record content items.

Classification guides (and their associated topics) enable convenient implementation of multiple classification schemes. They are used to define default values for the following classification-related metadata fields on the content check-in page:

❖ **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 records easier and more consistent, with similar records having the same classification metadata. You can further refine a classification guide by adding topics within a guide. See Creating or Editing a Classification Topic (page 6-41) for complete details.

To create a classification guide, select **Configure—Classification—Configure Classification Guide** from the Configure Records Management Page (page 7-2). Click **Add**. Enter an ID and a guide name (description), and click **Create**. A "Successfully created classification guide" screen is displayed showing the identifier and name of the newly created classification guide. The screen also includes a Page menu, where you can edit or delete the current classification guide, or add topics to it. Click **OK** when done.

SYSTEM-WIDE CONFIGURATION

This section describes configuration procedures used by administrators to set up DoD Edition. Certain configuration procedures described here and in other chapters may also apply to other users if they have been given the appropriate rights. The required rights for each procedure are described in Chapter 7 (*General Configuration Options)*, where these procedures are discussed in detail.

The Configure Records Management Page (page 7-2) is used to configure most aspects of DoD Edition. To access this page, select **Configure Records Management** from the **Administration** tray.

The following list highlights several tasks accomplished by using options on this page. For complete details about all the options, see Configure Records Management Page (page 7-2) for details.

- Set the fiscal calendar used by your organization for financial and accounting purposes. You need to specify the start date of your fiscal year only once, unless your organization changes their fiscal start date or the start date varies from year to year.

  To set the calendar, specify the date the fiscal year begins for your organization in the **Start of Fiscal Calendar** box on the Configure Records Management Page (page 7-2).

- Configure e-mail notifications sent to users which indicate that records or non-record content items require reviewing or that a pending disposition event requires attention.

  To set one or more default notification recipients specify one or more users in the **Notify recipient** box who will be the default recipients for notifications. You can enter their user names separated by commas, or select one or more users from the dropdown list on the right. Click **Submit Update**.

- Enable user-friendly captioning. Select this check box to enable more user-friendly language for disposition rules and screening criteria. Clear this check box for standard DoD 5015 disposition and screening query language. The disposition captions are displayed in the Disposition Information page and Disposition Rule screen. The screening query language is displayed in the Criteria boxes of the screening pages. Note that user-friendly captions are used on most of the screen depictions in this guide.

- Enable supplemental markings (available for records only). This setting enables supplemental marking security on records, records folders, and records users. This check box must be selected to enforce user matching of at least one supplemental marking, and also to enable the Supplemental Marking definition field. For more information, see Supplemental Markings (page 6-3)

- Classified Security (available for records only). This setting enables the classified security feature as required for agencies conforming to the Chapter 4 Classified Records section of DoD 5015.2 specification. When enabled, the Security Classification Field is displayed in the Configuring the Root Nodes (page 7-12). Clear this check box if your agency or organization does not require this feature.

The Configure menu on this page contains many common configuration tasks such as setting up triggers, determining time periods to use at your organization, and creating retention schedules. Details about those configuration tasks can be found in the remaining chapters of this guide.

SETTING UP A RETENTION SCHEDULE

A retention schedule is an organized hierarchy of series, categories, and folders, which emables you to cluster records and non-record content items into similar groups, each with its own retention and disposition characteristics.

You can configure the root series nodes for your retention schedule on the Configure Root Nodes page. This page displays the top level parent node of the retention schedule. Options on this page let you view information about the root node series, generates a retention schedule report for the *entire* retention schedule under the root node or let you hide the entire retention schedule from all other users except those with the 'rmaadmin' role. For more information, see Hiding and Unhiding a Series (page 8-17). To access the Root Node page, select **Configure—Root Nodes** on the Configure Records Management Page (page 7-2).

This section discusses the tasks involved in setting up a retention schedule. It covers the following topics:

- Managing Your Retention Schedule (page 3-11)
- Creating a Series (page 3-12)
- Creating a Retention Category (page 3-12)
- Creating a Records Folder (page 3-12)

Managing Your Retention Schedule

Plan to set up separate retention schedules for record items and non-record content items. Disposition instructions for non-record content items are usually different than those for record items. It is simpler to track items when they are sorted into appropriate categories.

Records and non-record content items are filed directly into a retention category, and records can optionally be filed into a records folder under a retention category. The retention schedule is the top-most series root node. The top node is created automatically for you by the system. The remaining retention schedule objects—series or records folder or retention category —are created by the records administrator.

A series is an optional container created by the records administrator. A retention category is required, and it contains disposition instructions for processing content and records. A records folder is optional, and it also organizes records according to some commonality.

See Chapter 8 (*Setting Up a Retention Schedule)* for complete details about planning and implementing a retention schedule.

Creating a Series

If an organization has many retention categories, setting up some series can assist with managing the view of the retention schedule hierarchies. You can nest series within each other. Series are also useful for creating work-in-progress retention schedules because series can be hidden from users, which prevents records or non-record content item users from filing any records into the hidden series.

To create the series, open the **Browse Content** tray and click the **Retention Schedules** link. Navigate to the series level in which to create a series. From the main **Actions** list, click **Create Series**. Enter an identifier and a name for the series. Click **Create**. The series is displayed in both the Browse Content tray area and in the Retention Schedule list.

Creating a Retention Category

A retention category is a retention schedule object that has associated security settings and disposition instructions defined. Retention categories cannot be nested within other retention categories.

Note: If ACLs are on the retention category, the records user must also be on the ACL to view or access the retention category.

To create a category, open the **Browse Content** tray and click the **Retention Schedules** link. Select **Create—Create Retention Category** from the Page menu. Configure the necessary information for the category. Several fields are optional. Required fields are indicated by red typeface on the Create Retention Category screen.

When done, click **Create**. The Dispositions Instructions page is displayed so you can create a disposition rule. To create a rule later, click **Submit Update**.

For detailed instructions about disposition rules and disposition examples, see Configuring Content Triggers, Dispositions, and Freezes (page 3-13) and Chapter 14 (*Defining Disposition Instructions)*.

Creating a Records Folder

Records have different metadata than content in the content server and are also associated with a disposition life cycle. A records folder organizes similar records within a retention category.

Multiple records folders can be stored in a category or can be nested within other records folders. Folders inherit disposition rules and security settings from their parent records folder or category but can also have their own rule or setting. You can also set supplemental markings on a records folder and on users to further secure the folder.

Records folders also inherit review information from their parent category. The review information that takes precedence is at the lowest node (the shortest review period prevails), as in the case of nested folders.

Records folder objects are unique because the records folders for temporary records are destroyed with the records. The records folders also have a life cycle that parallels that of its records. Records folders must be recreated on a regular basis, a practice that is not typically true of records series or categories in the retention schedule.

See Managing Records Folders (page 8-31) for complete details about tasks invinvoled in managing records folders. Also see the *Records Manager DoD Edition System Maintenance Guide* for other folder task information.

To create a records folder, first create a retention category and configure the time periods needed for dispositions. If necessary, also first create any supplemental markings that will be used. Open the retention category or records folder in which to create a records folder. From the main **Actions** list, click **Create Records Folder**. Configure the options for the folder. Several fields are optional. Required fields are indicated by red typeface on the Create Retention Folder screen.

CONFIGURING CONTENT TRIGGERS, DISPOSITIONS, AND FREEZES

Other retention elements can be configured to help you manage your record content. Triggers are used to initiate the disposition of content in a specified way and at specified periods of time. Freezes can be applied to content as needed. Content can be kept ‘frozen’ for specified amounts of time.

This section provides an overview of triggers, dispositions and freezes. For complete details, see Chapter 9 (*Setting up Triggers)*, Chapter 12 (*Configuring Dispositions and Freezes)* and Chapter 14 (*Defining Disposition Instructions)*.

This section covers the following topics:

- Triggers (page 3-14)
- Dispositions (page 3-14)
- Freezes (page 3-16)

Triggers

Two types of triggers can be used to initiate disposition processing:

- ❖ System derived triggers are built-in triggers based on defined events such as a preceding action, retention period cutoff, or a change in record states.
- ❖ Custom triggers can be created by administrators to define specific events. A custom trigger can affect all eligible records or non-record content items within a given retention category; whereas a system-derived trigger may only affect one record or non-record content item within a retention category, because it may be the only item that is in a given state. You can define three types of custom triggers:
  - Global triggers, which ocur at a defined time
  - Custom direct triggers, which use metadata fields as triggering events
  - Custom indirect triggers, which occur on a regular schedule

Custom triggers appear in the Triggering Events list of the Disposition Rules screen. For further information, see Chapter 14 *(Defining Disposition Instructions)*.

Select **Configure—Triggers** from the Configure Records Management Page (page 7-2). Select the type of trigger to create (Global Trigger, Custom Direct, or Indirect). Click **Add**. Configure the different options associated with the trigger. See Creating or Editing a Trigger (page 9-6) for complete details about the different custom trigger types and how to add them.

Dispositions

Dispostions are predefined actions taken on content, usually for items no longer needed for current business. See Chapter 12 *(Configuring Dispositions and Freezes)* for details.

A disposition is defined using instructions. An instruction usually follows this sequence:

> When a ***triggering event*** occurs, wait a specified ***rentention period***, then perform a specified ***action***.

Instructions are created within retention categories. Child records folders and records and non-record content items inherit dispositions from their parent retention category, but you can apply a disposition rule to a specific records folder only. You can use the built-in disposition actions provided with your system or create your own.

Disposition Types

The following types of dispositions are available:

- An *event disposition* is used when items are eligible for disposition when an event takes place. The event itself acts as a cutoff or closing occurrence.
- 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 record or content item.
- A *time-event disposition* is a disposition instruction that begins with a specified triggering event. After the event has transpired, then the folder, record, or non-record content item is cut off and the retention period is applied.

Triggering Events

A disposition instruction is activated when a ***triggering event*** occurs. Events can be split into general categories:

- those based on a preceding action
- those based on a record or content state
- those based on an indirect trigger
- those based on a custom trigger

Each category has several different events. For example, record or content states include the Activated triggering event, the Delete Approved triggering event, Superseded triggering event, No Longer Latest Revision triggering event, and so on.

See Triggering Events (page 14-5) for a complete list of triggering actions.

Retention Periods

The retention period is the interval of time after the triggering event before a disposition action is performed. Built-in period units are available or you can also create your own (see Creating or Editing a Custom Time Period (page 10-3)).

Disposition Actions

A disposition action defines what happens after Triggering Events (page 3-15) occur and Retention Periods (page 3-15), if any, have passed. Several built-in disposition actions are available or you can create your own.

Important: Records Manager DoD Edition does not perform the disposition action itself; rather, it sends an e-mail notification to the person responsible for carrying out the action.

Actions can be separated into several categories:

- ***General Actions:*** these include archive, cutoff, delete old revisions, no action, and so on.
- ***Non-Record Actions***: these include Delete Previous Revision, Delete Revision, and so on.
- ***Record Actions***: these include Accession, Destroy, Expire, and so on.
- ***Classified Actions***: these include declassify, upgrade, or downgrade classification.

Disposition Rules

After configuring the types of dispositions, you need to establish the rules used by the dispositions when evaluating content. Rules apply to all non-record content, records, and record folders in a category by default. You can also create a disposition rule that applies only to a specific records folder. See Disposition Examples (page 14-16) for specific procedures detailing different types of rules.

Freezes

Freezing a record, non-record content item, or records folder inhibits disposition processing. In addition, metadata for the folder, record, or item is also frozen.

You can predefine freeze types in order to better control the freeze/hold process. See Chapter 12 (*Configuring Dispositions and Freezes)* for details.

Chapter

4

DoD Edition Interface

Overview

This chapter describes the key elements of the product interface. It covers the following topics:

- Interface Overview (page 4-1)
- Individual Action Menus (page 4-3)

Interface Overview

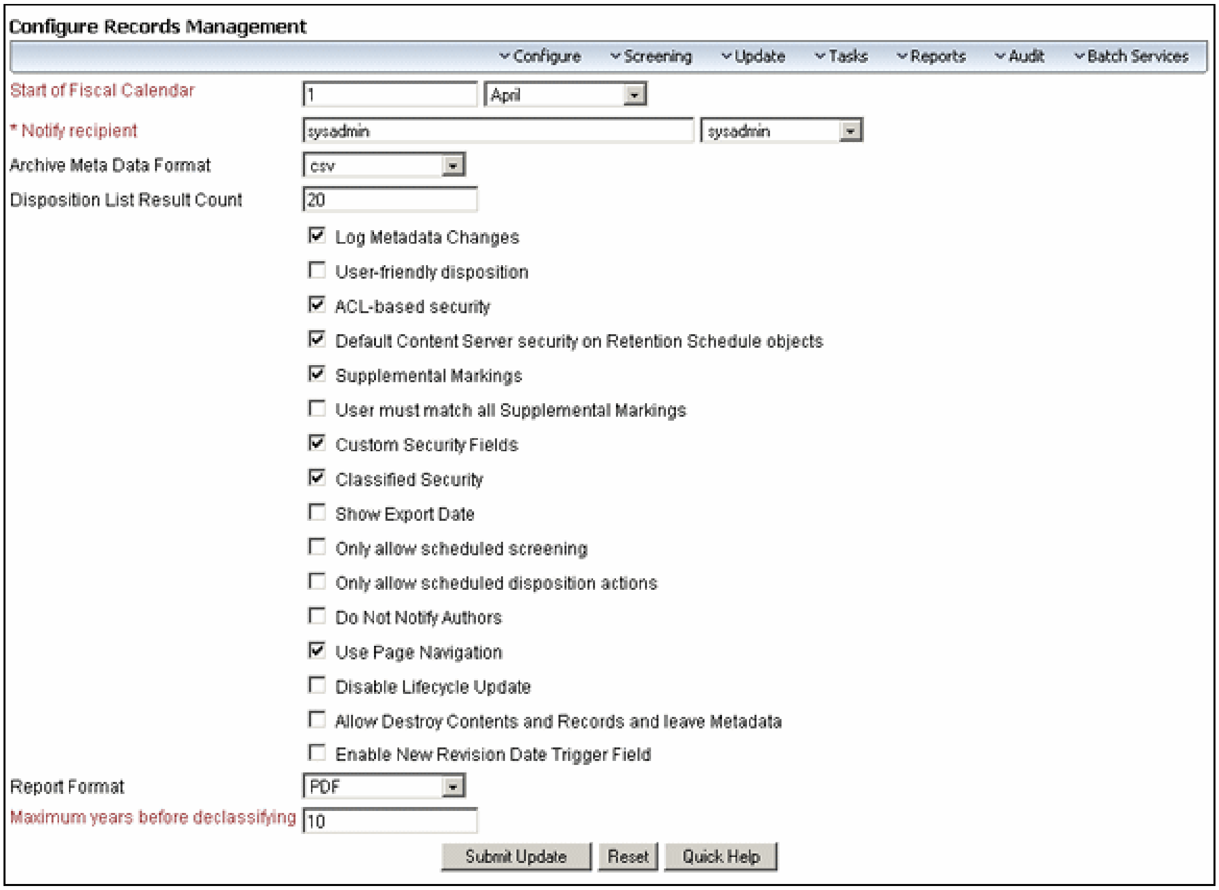
When DoD Edition is installed, a link to the Configure Records Management Page (page 7-2) is added to the **Administration** tray in the left navigation area of the Tray layout. Administrative users will see all options on that page. Other users (for example, those assigned privileged roles) may see a much smaller subset of the administrator menu, depending on their assigned rights.

Note: The exact menu options that any user sees depend on the rights assigned to that user. See Assigning Rights to User Roles (page 5-19)).

Use this page to set most of the configuration options for your system. To access this page, select **Configure Records Management** from the **Administration** tray.

Permissions: The Admin.RecordManager right is required to use this page. This right is assigned by default to the ‘rmaadmin’ role.

Figure 4-3 Configure Records Management page



Configure Records Management

Start of Fiscal Calendar	1 April
* Notify recipient	sysadmin sysadmin
Archive Meta Data Format	csv
Disposition List Result Count	20

☑ Log Metadata Changes
☐ User-friendly disposition
☑ ACL-based security
☑ Default Content Server security on Retention Schedule objects
☑ Supplemental Markings
☐ User must match all Supplemental Markings
☑ Custom Security Fields
☑ Classified Security
☐ Show Export Date
☐ Only allow scheduled screening
☐ Only allow scheduled disposition actions
☐ Do Not Notify Authors
☑ Use Page Navigation
☐ Disable Lifecycle Update
☐ Allow Destroy Contents and Records and leave Metadata
☐ Enable New Revision Date Trigger Field

Report Format	PDF
Maximum years before declassifying	10

See Configure Records Management Page (page 7-2) for details about using this page. The following is an overview of the options on the page:

❖ Top Page Menu: This menu contains the following options:

- **Configure:** This option is used to perform a number of configuration tasks, including defining triggers, periods, supplemental markings, security classifications, freezes, dispositions, custom security fields (if enabled on the Configure Records Management Page (page 7-2), custom metadata, and related content types. Other users may be able to perform a subset of these tasks, depending on their assigned rights.
- **Screening**: This option is used to perform a variety of screening operations, including screening by retention category, screening by records folder, screen by content,and other screening options. For further information about screening, see the *Records Manager DoD Edition Maintenance Guide*.

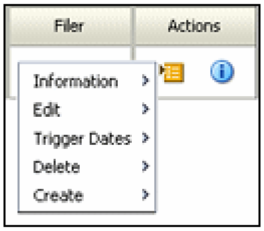
- **Update**: This option is only available if the noRmaSecurity right is enabled. It is used to generate updates to internal content, records folders, and retention categories. With this option you can quickly change multiple values, either immediately or on a scheduled basis. For more information, see the *Records Manager DoD Edition Maintenance Guide*.
- **Tasks**: This option is used to perform disposition actions, freezes, import and export files, and create reports. For further information about processing retention assignments, see the *Records Manager DoD Edition Maintenance Guide*.
- **Reports**: This option is used to generate a variety of reports, including users, users and their roles, aliases, and a combination of users and aliases. For further information about reports, see the *Records Manager DoD Edition Maintenance Guide*.
- **Audit**: This option lets administrative users specify what actions on content and records objects should be recorded in the audit trail and what should be used in audit trails.
- **Batch Services**: These options allow administrative users to run scheduled batch services immediately, rather than wait for the scheduled time. Options are used to run all batch services, process notifications, or process actions and reviews.

❖ **Main body:** This portion of the page is used to configure a number of system preferences, including security options, fiscal calendar start date, e-mail notifications of pending reviews, and user-friendly captions for disposition instructions and screening queries.

INDIVIDUAL ACTION MENUS

When using this product, individual pulldown Action menus are available for many items.

Figure 4-4 Actions menu



The options on this menu vary depending on the type of item used (content, retention category, and so on). In this documentation, a designation such as **Information—Recent**

Reviews indicates you should select the **Information** option from the **Actions** menu, followed by selecting the **Recent Reviews** suboption.

The following list summarizes the most commonly seen menu options:

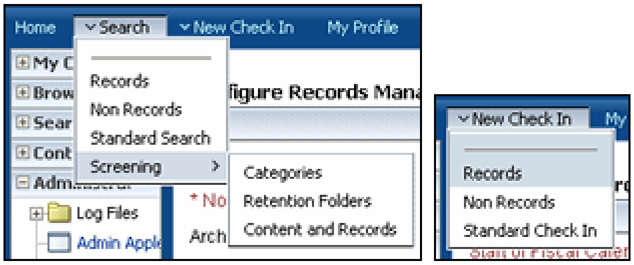
- **Information**: displays a submenu that allows you to access information pages for folders, life cycle of the item, recent reviews, metadata history, and retention schedule reports.
- **Edit**: provides quick links to edit pages for folders or reviews, as well as options to move, close, freeze, or unfreeze an item.
- **Trigger Dates**: provides quick links to actions associated with dates, such as marking items for review, cancelling, rescinding, and expiring items.
- **Delete**: provides options to delete the item or perform a recursive delete (delete tree).
- **Create**: provides options to create items appropriate to the location in the hierarchy. For example, if this is the action menu for a retention category, Create suboptions include Series and Retention Category.

Clicking the Info icon (ⓘ) displays the Information page for the item. The Action menu options described previously are then available on the Page menu on the item's information page.

Content Server Menus

When you install Records Manager DoD Edition the Search and Checkin menus for Content Server are changed due to default profile pages.

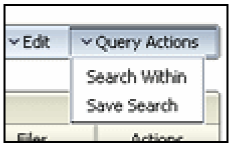
Figure 4-5 Additional Menu Options



These menu options can be used to help you quickly narrow down your searches and choose the type of checkin to perform. Note that the Screening option on the Search menu is dependent on security rights assigned to the user.

When viewing search results, a query menu is added to the search results page.

Figure 4-6 Query Menu on Search Results



The options on this menu let you narrow your search by selecting new fields from those already selected, or to save the search under a file name for use later. See the *Content Server User Guide* for more details about searching and saving query results.

You can change profiles and further refine options by using the **Configure—Profile—Profile <type>** option on the Configure Records Management Page (page 7-2).

Chapter

5

SETTING UP SECURITY

OVERVIEW

There are multiple layers of security in DoD Edition, including roles, rights, security grups, and access control lists. As with the standard content server security model, the final determination of permissions and privileges is determined by the intersection of all security mechanisms in place. The strictest setting prevails.

Access control lists and supplemental markings are required for compliance by DoD Edition with the DoD 5015.2 specification. Classification levels are required for compliance with Chapter 4 of DoD 5015.2. See Chapter 6 *(Additional Security Settings)* for details.

You can also use Content Server's accounts security model in addition to the options provided by DoD Edition. For more information about the account security model, see the Content Server administrator documentation.

This section covers the following topics:

Concepts

- ❖ Records Management in an Organization (page 5-2)
- ❖ Roles (page 5-3)
- ❖ Rights (page 5-4)
- ❖ Security Groups (page 5-16)
- ❖ Access Control Lists (ACLs) (page 5-16)
- ❖ Records Objects Security Matrix (page 5-17)

Tasks

- Setting Security Preferences (page 5-18)
- Assigning Rights to User Roles (page 5-19)

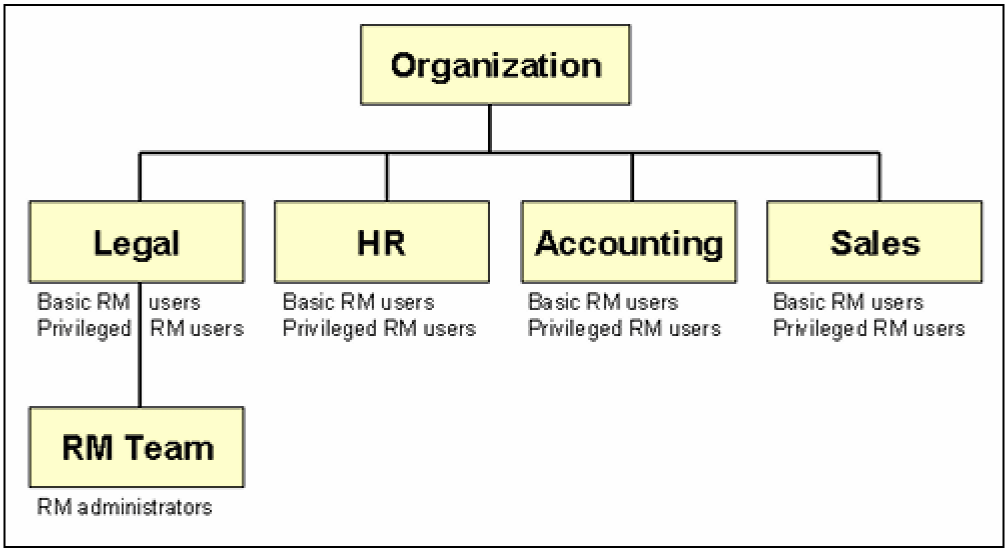
Interface

- Edit RMA Rights Screen (page 5-20)

Records Management in an Organization

The figure below shows a typical records management structure in an organization.

Figure 5-7 Typical records management organization



Most people in the various departments of an organization can file a record or check in a non-record content item, search for it, and view it. They are the basic records management (RM) users.

A much smaller group of people is typically granted rights to perform some additional functions not allowed for basic users (for example, creating triggers or retention schedules).

A very limited number of people are records administrators, who are typically responsible for setting up and maintaining the records management infrastructure. Records administrators have the widest range of rights to perform records management tasks. For example, they can usually perform *all* records and disposition actions, including those assigned to others. The records administrators are often in the legal department of an organization, which can drive the efforts for effective and efficient records management.

DoD Edition comes with predefined records management roles called ‘rma’, ‘rmaprivileged’, and ‘rmaadmin’. 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. However, these roles can easily be modified to suit specific records management needs. You can also create new roles and assign records management rights to them, or grant records management rights to existing Content Server roles.

Users without specific records rights can still apply lifecycle to non-record content items.

Important: Records management consists of more than just software. You also need to have the appropriate organizational structures and policies in place in your organization.

ROLES

DoD Edition comes with three predefined user roles, discussed in detail in Security Groups (page 5-16):

- **rma:** This role is generally assigned to basic records users. It allows them to perform basic records management tasks. Users with this role have read permission (R) to the Public security group, as well as read and write permission (RW) to the special Record Group security group.
- **rmaprivileged:** This role is generally assigned to “privileged” users, who have all the permissions that basic records users (‘rma’ role) have, but are also granted rights to perform additional functions (for example, creating triggers or folders, and modifying record attributes).

  Users with the ‘rmaprivileged’ role have read permission (R) to the Public security group, as well as read and write permission (RW) to the special Records Group security group.
- **rmaadmin:** This role is generally assigned to records administrators, who are responsible for setting up and maintaining the records management infrastructure and environment. These users have the widest range of rights to perform records management tasks (for example, defining users this role to have read permission (R) to the Public security group, as well as read, write, delete, and write permission (RWDA) to the special Records Group security group).

Each of these predefined roles comes with a default set of permissions and rights, but these can be modified to suit your specific needs. You can also create new roles and assign records management rights to them, or grant records management rights to existing Content Server roles. This enables you to define a very granular security model for your records management environment.

Note: Role permissions are additive, just as in Content Server. If your organization uses accounts, the accounts are a hierarchical overlay to your current security model.

RIGHTS

Access to the majority of functions is controlled by rights that are assigned to Content Server user roles. The three predefined records management roles ('rma', 'rmaprivileged', and 'rmaadmin') each have a default set of rights assigned to them, but the roles can easily be modified to restrict or expand their access to records management functions (see Assigning Rights to User Roles (page 5-19) for details).

If the Related Content component is installed, the Record.CreateLink and Record.Unlink rights are set by default for users.

Note: The ability to browse and view the retention schedule not only depends on assigned rights, but also on any other applied security features, such as supplemental markings and access control lists (ACLs). See Chapter 8 *(Setting Up a Retention Schedule)* for details about retention schedules. See Chapter 6 *(Additional Security Settings)* and Access Control Lists (ACLs) (page 5-16) for further details.

The following table gives more detailed information about tasks that can be performed in DoD Edition and the rights required to perform each task. See each designated chapter for further details about the specific permissions required for individual tasks.

Function	**Required RM Right**	**Defaults for Predefined RM Roles**		
		rma	**rmaprivileged**	**rmaadmin**
TRIGGERS. See Chapter 9 *(Setting up Triggers)*				
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

Function	Required RM Right	Defaults for Predefined RM Roles		
		rma	rmaprivileged	rmaadmin
Delete a trigger	Admin.Triggers *and* Delete permission for the trigger's security group		X (Delete permission not granted by default)	X
PERIODS. See Chapter 10 (*Configuring Time Periods)*				
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
SUPPLEMENTAL MARKINGS. See Chapter 6 (*Additional Security Settings)*				
View information about supplemental markings	Admin.Triggers or Admin.RecordManager		X	X
Enable supplemental markings	Admin.RecordManager			X
Disable supplemental markings	Admin.RecordManager			X
Create a supplemental marking	Admin.RecordManager			X
Edit a supplemental marking	Admin.RecordManager			X
Delete a supplemental marking	Admin.RecordManager			X
SECURITY CLASSIFICATIONS. See Chapter 6 (*Additional Security Settings)*				
View information about security classifications	Admin.RecordManager *and* Admin.SecurityClassifications			X

Function	Required RM Right	Defaults for Predefined RM Roles		
		rma	rmaprivileged	rmaadmin
Enable security classifications	Admin.RecordManager *and* Admin.SecurityClassifications			X
Disable security classifications	Admin.RecordManager *and* Admin.SecurityClassifications			X
Create security classifications	Admin.RecordManager *and* Admin.SecurityClassifications			X
Edit security classifications	Admin.RecordManager *and* Admin.SecurityClassifications			X
Delete security classifications	Admin.RecordManager *and* Admin.SecurityClassifications			X
Reorder security classifications	Admin.RecordManager *and* Admin.SecurityClassifications			X
CUSTOM SECURITY FIELDS. See Custom Security Fields (page 6-27)				
View information about custom security field	Admin.Triggers or Admin.RecordManager		X	X
Enable custom security fields	Admin.RecordManager			X
Disable custom security fields	Admin.RecordManager			X
Create a custom security field	Admin.RecordManager			X
Edit a custom security field	Admin.RecordManager			X
Delete a custom security field	Admin.RecordManager			X
CUSTOM CATEGORY OR FOLDER METADATA FIELDS. See Chapter 11 (*Custom Metadata Fields)*				
Create custom category or folder metadata field	Admin.RecordManager			X

Function	Required RM Right	Defaults for Predefined RM Roles		
		rma	rmaprivileged	rmaadmin
Edit custom category or folder metadata field	Admin.RecordManager			X
Delete custom category or folder metadata field	Admin.RecordManager			X
CLASSIFICATION GUIDES. See Classification Guides (page 6-37)				
View information about classification guides	Admin. ClassificationGuide		X	X
Create classification guide	Admin. ClassificationGuide		X	X
Edit classification guide	Admin. ClassificationGuide		X	X
Delete classification guide	Admin. ClassificationGuide		X	X
View information about classification topic	Admin. ClassificationGuide		X	X
Create classification topic	Admin. ClassificationGuide		X	X
Edit classification topic	Admin. ClassificationGuide		X	X
Delete classification topic	Admin. ClassificationGuide		X	X
FREEZES. See Freezes (page 12-14)				
View information about freezes	Admin.RecordManager			X
Creating freezes	Admin.RecordManager			X

Function	Required RM Right	Defaults for Predefined RM Roles		
		rma	rmaprivileged	rmaadmin
Edit freezes	Admin.RecordManager			X
Delete freezes	Admin.RecordManager *and* Delete permission for the freeze's security group			X
Sending e-mail notifications about freezes	Admin.RecordManager			X
SERIES. See Using a Series (page 8-15)				
Browse and view information about a series	Series.Read	X	X	X
Create a series	Series.Create			X
Edit a series	Series.Edit			X
Hide a series	Series.Hide/Unhide			X
Unhide a series	Series.Hide/Unhide			X
Move a series	Series.Move			X
Delete a series	Series.Delete			X
CATEGORIES. See Retention Categories (page 8-21)				
Browse and view information about retention categories (including disposition instructions)	Category.Read	X	X	X
Create a retention category	Category.Create			X
Edit a retention category	Category.Edit			X
Edit the review information for a retention category	Category.EditReview			X

Function	**Required RM Right**	**Defaults for Predefined RM Roles**		
		rma	**rmaprivileged**	**rmaadmin**
Move a retention category	Category.Move			X
Delete a retention category	Category.Delete			X
Apply/reapply disposition rules to specific/all records and non-record content items in a retention category	Category.Edit			X
FOLDERS. See the *Records Manager DoD Edition System Maintenance Guide*				
Browse and view information about records folders	Folder.Read	X	X	X
View the life cycle of a records folder	Folder.Read	X	X	X
View the review history of a records folder	Folder.Read	X	X	X
View the metadata history of a records folder	Folder.Read	X	X	X
Create a records folder	Folder.Create		X	X
Edit a records folder (if the user is the author of that folder)	Folder.EditIfAuthor		X	
Edit a records folder (if the user is *not* the author of that folder)	Folder.Edit			X
Edit the review information of a records folder	Folder.EditReview		X	X
Move a records folder	Folder.Edit			X
Delete a records folder	Folder.Delete			X

Function	Required RM Right	Defaults for Predefined RM Roles		
		rma	rmaprivileged	rmaadmin
Close a records folder	Folder.Open/Close		X	X
Unclose a records folder	Folder.Open/Close		X	X
Freeze a records folder	Folder.Freeze/Unfreeze			X
Unfreeze a records folder	Folder.Freeze/Unfreeze			X
Cancel a records folder	Folder.Edit		X	X
Expire a records folder	Folder.Edit		X	X
Rescind a records folder	Folder.Edit		X	X
Make a records folder obsolete	Folder.Edit		X	X
Undo the obsolete status of a records folder	Folder.Edit		X	X
Undo the cutoff of a records folder	Folder.UndoCutoff			X
Review a records folder	Admin. PerformPendingReviews		X	X
Mark a records folder as reviewed	Folder.Edit		X	X
Set activation, expiration, delete, and approval dates for records folders	Folder.Edit		X	X
Assign supplemental markings to a records folder	Folder.Edit		X	X
Remove supplemental markings from a records folder	Folder.Edit		X	X

Function	**Required RM Right**	**Defaults for Predefined RM Roles**		
		rma	**rmaprivileged**	**rmaadmin**
Apply a disposition rule to a specific records folder	Category.Edit			X
Apply a disposition rule to all records folders	Category.Edit			X
CONTENT. See the *Records Manager DoD Edition System Maintenance Guide*				
Download a record or non-record content item for viewing	Record.Read	X	X	X
View information about a record or non-record content item	Record.Read	X	X	X
View the life cycle of a record or non-record content item	Record.Read	X	X	X
View the review history of a record or non-record content item	Record.Read	X	X	X
View the metadata history of a record or non-record content item	Record.Read	X	X	X
View the classification history of a record	Record.Read	X	X	X
Edit the review information for a record or non-record content item	Record.EditReview		X	X
Review the classification of a record	Record.Edit		X	X

Function	Required RM Right	Defaults for Predefined RM Roles		
		rma	rmaprivileged	rmaadmin
Delete the metadata history of a record or non-record content item	Record.DeleteHistoryFile		X	X
Create a record or check in a non-record content item	Record.Create	X	X	X
Search for records or non-record content items	Record.Read	X	X	X
Link records or non-record content items	Record.CreateLink	X	X	X
Unlink records or non-record content items	Record.Unlink		X	X
Delete a record or non-record content item	Record.Delete			X
Freeze a record or non-record content item	Record.Freeze/Unfreeze			X
Unfreeze a record or non-record content item	Record.Freeze/Unfreeze			X
Cancel a record or non-record content item	Record.Edit		X	X
Expire a record or non-record content item	Record.Edit		X	X
Rescind a record or non-record content item	Record.Edit		X	X
Make a record or non-record content item obsolete	Record.Edit		X	X

Function	Required RM Right	Defaults for Predefined RM Roles		
		rma	rmaprivileged	rmaadmin
Undo the obsolete status of a record or non-record content item	Record.Edit		X	X
Move a record to another category or folder. Move a non-record content item to another category.	Record.Edit		X	X
Edit record metadata before a cutoff. **Note**: You can edit metadata for non-record content items after cutoff as well as before cutoff.	Record.UndoCutoff			X
Upgrade or downgrade the security classification of a record	Record.Upgrade/Downgrade		X	X
Review a record or non-record content item	Admin. PerformPendingReviews		X	X
Remove a supplemental marking from a record	Record.Edit		X	X
Undo the cutoff of a record or non-record content item	Record.UndoCutoff			X
Undo the record status of a content item	Record.UndoRecord			X
DISPOSITION RULES. See Chapter 14 (*Defining Disposition Instructions)*				
View disposition information	Category.Read	X	X	X
Enable/disable user-friendly disposition captions	Admin.RecordManager			X

Function	**Required RM Right**	**Defaults for Predefined RM Roles**		
		rma	**rmaprivileged**	**rmaadmin**
Create disposition rules	Category.Create			X
Edit disposition rules	Category.Edit			X
Delete disposition rules	Category.Delete			X
Define custom disposition actions	Admin.CustomDisposition Actions			
ARCHIVING. See the *Records Manager DoD Edition System Maintenance Guide*				
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
SCREENING. See the *Records Manager DoD Edition System Maintenance Guide*				
Enable/disable advanced screening	Admin.Screening			X
Enable/disable user-friendly screening captions	Admin.RecordManager			X
Screen retention categories	Admin.Screening			X
Screen records folders	Admin.Screening			X
Screen records and non-record content	Admin.Screening			X
AUDIT TRAILS. See the *Records Manager DoD Edition System Maintenance Guide*				
Configure the audit trail	Admin.Audit			X
Select what metadata fields to include in the audit trail	Admin.SelectMeta			X

Function	Required RM Right	Defaults for Predefined RM Roles		
		rma	rmaprivileged	rmaadmin
Generate and view an audit trail	Admin.Audit			X
Search with audit trails	Admin.Audit			X
Set default metadata for checking in audit trails	Admin.Audit			X
Check in and archive audit trails	Admin.Audit			X
Search archived audit trails	Admin.Audit			X
LINKS. See Chapter 13 (*Configuring Related Content (Links)*)				
Add custom link types	Admin.ConfigureLinkTypes			X
Edit custom link types	Admin.ConfigureLinkTypes			X
Delete custom link types	Admin.ConfigureLinkTypes			X
Create links between records and non-record content items	Record.CreateLink		X	X
Remove links between records and non-record content items	Record.Unlink		X	X
GENERATING REPORTS. See the *Records Manager DoD Edition System Maintenance Guide*				
Create a user group	Admin.Reports			X
Create a role report	Admin.Reports			X
Create a group report	Admin.Reports			X
Create a user-group report	Admin.Reports			X
OTHER TASKS				
Configure the root nodes	Admin.RecordManager			X

Function	Required RM Right	Defaults for Predefined RM Roles		
		rma	rmaprivileged	rmaadmin
Setting the fiscal calendar	Admin.RecordManager			X
Perform disposition actions (processing events)	Admin.PerformActions			X
Specify the default recipient(s) for notifications	Admin.RecordManager			X

Those entries marked with an asterisk (*) indicate tasks which a user can perform outside the retention schedule without any specific retention role rights.

Note: The previous table outlines the default configuration. The security model is highly customizable, which means that it can be modified to suit the needs of your specific environment.

Security Groups

DoD Edition comes with a predefined security group called “RecordsGroup.” A security group defines security on a group of content. In the case of records management, the RecordsGroup security group defines security for a group of content designated as records.

Users with the predefined ‘rma’ or ‘rmaprivileged’ roles have read and write permission (RW) to the RecordsGroup security group. Users with the ‘rmaadmin’ role have read, write, delete, and admin permission (RWDA) to this security group.

Note: Even though the default ‘rma’ and ‘rmaprivileged’ roles appear to be identical, they are not. The default ‘rmaprivileged’ role has subadministrator access to certain administrator functions that the default ‘rma’ role does not—for example, creating triggers and records folders, or editing records. For details about rights that can be assigned to roles, see Rights (page 5-4).

Access Control Lists (ACLs)

Access control lists (ACLs) are intended to manage the security model on dispositions. You can assign ACLs to the following retention schedule components:

- triggers
- retention categories
- records folders

You can use ACLs to control user and group access permissions for triggers, categories, and records folders. You can assign the ACL for each category, records folder, and trigger you create.

Searching for records and non-record content items takes more time when using ACLs because the permissions are checked on all parent records folders and categories for a record. ACLs do not affect the search performance when searching for non-record content in Content Server.

If your organization is not required to use ACLs, you might want to consider disabling ACLs for faster search retrieval performance. If your organization is not required to comply with this specification, the content server security, custom security fields, and supplemental markings also provide excellent security.

Records Objects Security Matrix

The table below shows a matrix of records, non-record content and retention schedule components, and the corresponding permissions for each predefined role. Supplemental markings have the most restrictive records access capabilities. See Chapter 6 (*Additional Security Settings)* for details.

Objects and Retention Schedule Components	**Subject to Additional Security of Type**	**basic user (rma)**	**privileged (rmaprivileged)**	**administrator (rmaadmin)**
Records/Non-record 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	R	R	RWD

Objects and Retention Schedule Components	Subject to Additional Security of Type	basic user (rma)	privileged (rmaprivileged)	administrator (rmaadmin)
Triggers	Rights; ACLs		RW **Note:** RWD permission required to delete triggers.	RWDA **Note:** Only custom triggers can be deleted.
Periods	Rights		R	RWD **Note:** Only custom periods can be deleted.
Supplemental markings	Rights			RWD
Classification guides	Rights			RWD

Setting Security Preferences

Security preferences are set on the Configure Records Management Page (page 7-2). The security preferences set on that page are in addition to those provided with the standard Stellent content server.

Caution: After your production environment is underway, it is recommended that you do not change the security settings for ACLs or the default Content Server security.

To configure security settings for DoD Edition, complete the following steps:

1. Select **Configure Records Management** from the **Administration** tray.

   The Configure Records Management Page (page 7-2) is displayed.

2. (Optional based on your security model): To make use of Access Control List Security, select the **ACL-based security** check box.

3. (Recommended): To activate the default security inherent in Universal Content Management for extra security on categories, folders, and triggers, select the **Default Content Server security on Categories, Folders, and Triggers** check box. To not set the additional security on categories, records folders, and triggers, clear the check box.

4. (Required for DOD 5015.2 compliance): To use supplemental markings, select the **Supplemental Marking** check box. For the strictest setting, also select the **User must match all Supplemental Markings** check box. For more information, see Supplemental Markings Details (page 6-3).
5. (Optional based on your security model): To make users match all supplemental markings on a records folder to access a record, select the **User must match all Supplemental Markings** check box. This is the most restrictive setting for supplemental markings. To allow a user to match only one supplemental marking to a records folder or record (in the case of multiple supplemental markings) to access its records, clear the check box.
6. (Optional): To create your own custom security fields at the content field level that further restricts users, select the **Custom Security Fields** check box. To not use custom security fields, clear the check box.
7. (Optional): To use classified record security, select the **Classified Security** check box. To not use classified security fields, clear the check box. For more information, see About Records Classification (page 6-14).
8. Click **Submit Update**. A message is displayed saying that records management has been configured successfully.

ASSIGNING RIGHTS TO USER ROLES

Records Manager DoD Edition comes with three predefined roles: ‘rma,’ ‘rmaprivileged,’ and ‘rmaadmin.’ Each of these roles has a number of default rights, which define what users with that role are allowed to do. For further details about roles and their default rights, see Rights (page 5-4).

This section discusses the following topics:

- Setting Rights for Roles (page 5-19)
- Edit RMA Rights Screen (page 5-20)

Setting Rights for Roles

Rights define what actions users are allowed to perform on record or non-record content items. To assign rights to user roles, complete the following steps:

1. Select **Admin Applets** from the **Administration** tray.

The Administration Applets page for your server is displayed.

2. Click the **User Admin** icon.

   The User Admin utility starts.

3. Choose **Security—Permissions by Role** from the menu.
4. Select the DoD Edition role to review or modify. Click **Edit RMA Rights**.

   The Edit RMA Rights Screen (page 5-20) is displayed.

5. Set the appropriate rights by selecting or clearing the check boxes on the various tabs.
6. Click **OK** when you finish.
7. Click **Close** to exit the Permissions by Role screen.

Edit RMA Rights Screen

Use this screen to assign records management rights to Content Server and/or Records Manager roles. To access the Edit RMA Rights screen, complete the following steps:

1. Select **Admin Applets** from the **Administration** tray.

   The Administration Applets page for your server is displayed.

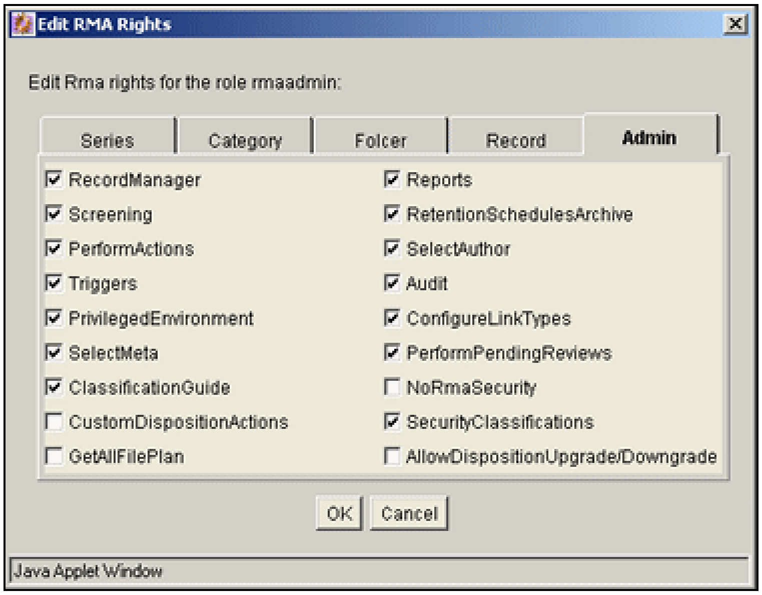
2. Click the **User Admin** icon.

   The User Admin utility starts.

3. Choose **Security—Permissions by Role** from the menu. Select a role to view the rights. In the following example, ‘rmaadmin’ was selected.
4. Click **Edit RMA Right.**

   The Edit RMA Rights screen is displayed.

Figure 5-8 Edit RMA Rights dialog



Edit Rma rights for the role rmaadmin:

☑ RecordManager
☑ Screening
☑ PerformActions
☑ Triggers
☑ PrivilegedEnvironment
☑ SelectMeta
☑ ClassificationGuide
☐ CustomDispositionActions
☐ GetAllFilePlan
☑ Reports
☑ RetentionSchedulesArchive
☑ SelectAuthor
☑ Audit
☑ ConfigureLinkTypes
☑ PerformPendingReviews
☐ NoRmaSecurity
☑ SecurityClassifications
☐ AllowDispositionUpgrade/Downgrade

Screen Features

The table below describes the features of the Edit RMA Rights screen, as well as the default rights for each of the predefined roles.

Note: 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 will be enabled automatically.

Feature	Description	Defaults Rights for Roles		
		rma	rmaprivileged	rmaadmin
SERIES TAB (see Using a Series (page 8-15))				
Read	If enabled, the user can view information about a series.	X	X	X
Create	If enabled, the user can create a series.			X

Feature	**Description**	**Defaults Rights for Roles**		
		rma	**rmaprivileged**	**rmaadmin**
Delete	If enabled, the user can delete a series.			X
Move	If enabled, the user can move a series.			X
Edit	If enabled, the user can edit a series.			X
Hide/Unhide	If enabled, the user hide and unhide a series.			X
CATEGORY TAB (See Retention Categories (page 8-21))				
Read	If enabled, the user can view information about a retention category.	X	X	X
Create	If enabled, the user can create a retention category.			X
Delete	If enabled, the user can delete a retention category.			X
Move	If enabled, the user can move a retention category.			X
Edit	If enabled, the user can edit a retention category.			X
EditReview	If enabled, the user can edit a retention category that is subject to review.			X
FOLDER TAB (see the *Records Manager DoD Edition System Maintenance Guide*)				
Read	If enabled, the user can view information about a records folder.	X	X	X

Feature	Description	Defaults Rights for Roles		
		rma	rmaprivileged	rmaadmin
Create	If enabled, the user can create a records folder.		X	X
Delete	If enabled, the user can delete a records folder.			X
Open/Close	If enabled, the user can open and close a records folder.		X	X
EditReview	If enabled, the user can edit a records folder that is subject to review.		X	X
Move	If enabled, the user can move a records folder.		X	X
Edit	If enabled, the user can edit a records folder, even if the user is not the author of that folder.			X
UndoCutoff	If enabled, the user can undo the cutoff of a records folder.			X
Freeze/Unfreeze	If enabled, the user can freeze and unfreeze a records folder.			X
EditIfAuthor	If enabled, the user can edit a records folder, but only if the user is the author of that folder.		X	
RECORD TAB (see the *Records Manager DoD Edition System Maintenance Guide*)				
Read	If enabled, the user can view information about a record or non-record content item.	X	X	X

Feature	Description	Defaults Rights for Roles		
		rma	rmaprivileged	rmaadmin
Edit	If enabled, the user can edit a record or non-record content item, including moving, cancelling, expiring, rescinding, making obsolete, and reviewing.		X	X
UndoCutoff	If enabled, the user can undo the cutoff of a record.			X
DeleteHistoryFile	If enabled, the user can delete the metadata history file of a record. This check box is only available if the 'Classified Security' option has been enabled on the Configure Records Management page.		X	X
EditReview	If enabled, the user can edit a record or non-record content item that is subject to review.		X	X
CreateLink	If enabled, the user can link records or non-record content items. See Chapter 13 (*Configuring Related Content (Links)*)	X	X	X

Feature	Description	Defaults Rights for Roles		
		rma	rmaprivileged	rmaadmin
NoPostFilterSearch	If enabled, the user can unfilter search results. The results include records and non-record content items that 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 record or non-record 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 needs to be performed. Users with this right can still only access non-record 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. However, they will see some metadata information about the record or non-record content item (for example, their title), which may interfere with your organization’s security model.			
Create	If enabled, the user can create a record or check in a non-record content item into the retention schedule. For details, see the *Records Manager DoD Edition User Guide*.	X	X	X

Feature	**Description**	**Defaults Rights for Roles**		
		rma	**rmaprivileged**	**rmaadmin**
Delete	If enabled, the user can delete a record or non-record content item within the retention schedule.			X
Freeze/Unfreeze	If enabled, the user can freeze and unfreeze a record or non-record content item.			X
Upgrade/Downgrade	If enabled, the user can upgrade and downgrade the security classification of a record. This check box is only available if the ‘Classified Security’ option has been enabled on the Configure Records Management page.		X	X
UndoRecord	If enabled, the user can undo the record status of a content item.			X
Unlink	If enabled, the user can unlink record or non-record content. See Configuring Related Content (Links) (page 13-1).	X	X	X
ADMIN TAB				
RecordManager	If enabled, the user can configure a number of settings in the record management environment and also set up and administer periods, supplemental markings, security classifications, custom security fields, custom category and folder metadata fields, classification guides and freezes.			X

Feature	**Description**	**Defaults Rights for Roles**		
		rma	**rmaprivileged**	**rmaadmin**
Screening	If enabled, the user can screen retention categories, records folders, and items. See the *Records Manager DoD Edition System Maintenance Guide*.			X
PerformActions	If enabled, the user can process record or non-record content assignments. See the *Records Manager DoD Edition System Maintenance Guide*.			X
Triggers	If enabled, the user can work with global triggers, custom direct triggers, and indirect triggers. See Chapter 9 (*Setting up Triggers)*. **Note:** To delete a trigger, you also need Delete permission (D) for the trigger's security group.		X (Delete permission not granted by default)	X
PrivilegedEnvironment	If enabled, the user can set the declassification timeframe (see Setting the Declassification Time Frame (page 6-20)). This check box is only available if the 'Classified Security' option has been enabled on the Configure Records Management Page (page 7-2)**.**		X	X
SelectMeta	If enabled, the user can specify which metadata fields should be audited.			X

Feature	Description	Defaults Rights for Roles		
		rma	rmaprivileged	rmaadmin
ClassificationGuide	If enabled, the user can work with classification guides.		X	X
CustomDispositionActions	If enabled, the user can define custom disposition actions. See Custom Disposition Actions (page 12-3).			
GetAllFilePlan	If enabled, this right allows the user to get all series, categories, and record folders when the GET_FILE_PLAN_ALL service is called. Without this right, unaccessible fileplan objects are excluded. The service is typically used by URM adapters.			
Reports	If enabled, the user can generate user and group reports. See the *Records Manager DoD Edition System Maintenance Guide*.			X
RetentionScheduleArchive	If enabled, the user can import and export a retention schedule archive. See the *Records Manager DoD Edition System Maintenance Guide*.			X
SelectAuthor	If enabled, the user can select a different filer (author) for a category or record than him/herself.			X
Audit	If enabled, the user can work with audit trials. See the *Records Manager DoD Edition System Maintenance Guide*.			X

Feature	Description	Defaults Rights for Roles		
		rma	rmaprivileged	rmaadmin
ConfigureLinkTypes	If enabled, the user can manage custom record or non-record content links. See the *Records Manager DoD Edition System Maintenance Guide*			X
PerformPendingReviews	If enabled, the user can perform pending reviews. See the *Records Manager DoD Edition System Maintenance Guide*.		X	X

Feature	**Description**	**Defaults Rights for Roles**		
		rma	**rmaprivileged**	**rmaadmin**
NoRmaSecurity	If enabled, the user becomes "immune" to security classifications, supplemental markings, custom security fields, and ACLs. Their access to records is unrestricted by these security features. In addition, this option turns off search post-filtering, so search results include records or non-record content items that the user has not been explicitly granted access to. For example, a user would have access to records marked as "Top Secret" even if that security classification has not been assigned to the user. This right can be used to give sysadmins the privilege to access every record or non-record content item in the system. **Note:** Access to record or non-record content items continues to be restricted by security groups and accounts.			

Feature	Description	Defaults Rights for Roles		
		rma	rmaprivileged	rmaadmin
SecurityClassifications	If enabled (with the Admin.RecordManager option), the user is allowed to set up security classification levels. See Security Classifications (page 6-13). This check box is only available if the 'Classified Security' option has been enabled on the Configure Records Management Page (page 7-2)			X *(new installs only)*
AllowDispositionUpgrade/ Downgrade	If enabled, allows the user to perform upgrade and downgrade classification actions.			X

Important: 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.

Chapter

6

ADDITIONAL SECURITY SETTINGS

OVERVIEW

This section describes how to use the classification, classification guides, and supplemental marking functions which can be used to provide additional security for your environment. It covers the following topics:

Concepts

Tasks

Examples

Interface

- Create or Edit Custom Security Field Page (page 6-35)
- Custom Security Field Information Page (page 6-37)
- Configure Classification Guide Page (page 6-44)
- Create or Edit Classification Guide Page (page 6-45)
- Classification Guide Information Page (page 6-46)
- Administer Classification Topic Page (page 6-47)
- Create or Edit Classification Topic Page (page 6-48)
- Classification Topic Information Page (page 6-51)
- Configure Topic Settings Page (page 6-50)

SUPPLEMENTAL MARKINGS

Supplemental markings can be assigned to records and records 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.” Supplemental markings can be set at both the records folder and the record level.

Note: Supplemental markings are available for record content only. They are not used with non-record content.

This section covers the following topics:

- Supplemental Markings Details (page 6-3)
- Managing Supplemental Markings (page 6-6)

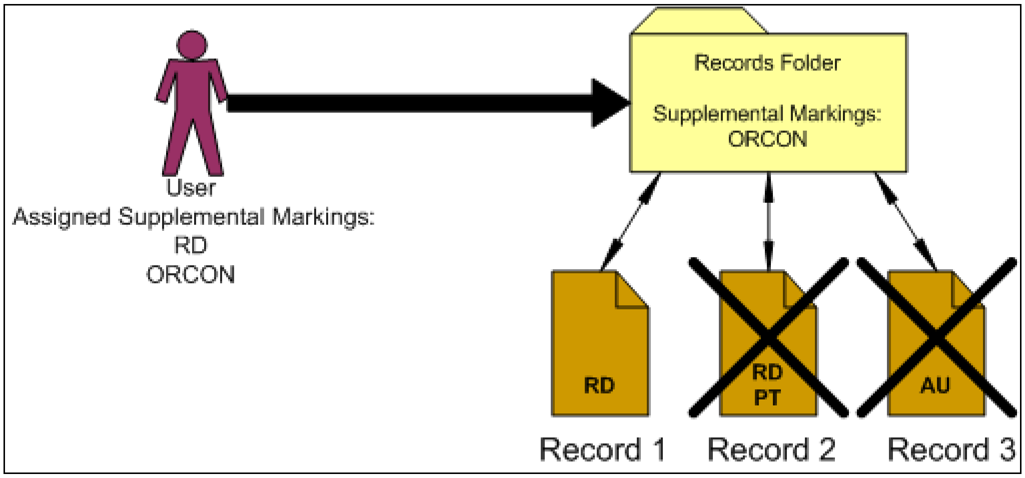
Supplemental Markings Details

In addition to using supplemental markings as a means of clarifying document handling, you can also use supplemental markings as a security feature to further restrict users from accessing records folders and records.

Note: To disable the use of supplemental markings as a security feature, clear the *Supplemental Markings* check box on the Configure Records Management Page and do not assign the markings to users.

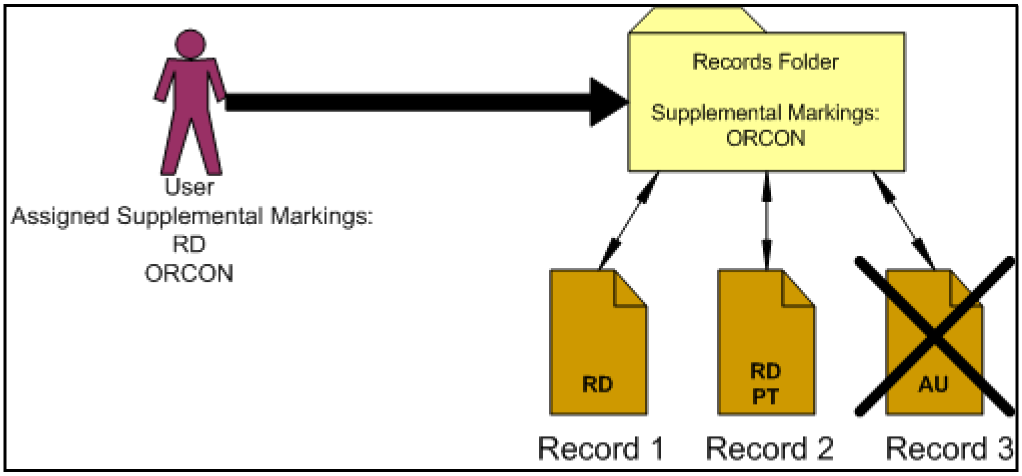
When you assign supplemental markings to users, even if a user has access to a specific records folder, the supplemental marking further restricts access to folders and records. In circumstances where a folder or record has multiple supplemental markings, you can require that a user match all assigned supplemental markings to access a record or records folder. Otherwise (that is, when 'match all' is disabled), if a user matches just one of the multiple supplemental markings, the user can access the record or records folder object.

Figure 6-9 User must match all supplemental markings



For example, in the diagram above, the records user is assigned the supplemental markings "RD" and "ORCON." The Records Folder is marked with "ORCON," therefore the user can access the folder. The records 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 "Record 1" marked with the supplemental marking "RD." Because the user has not been assigned the supplemental marking "PT" or "AU", the user cannot access "Record 2," which has the multiple markings "RD" and "PT," nor can the user access "Record 3" with the marking "AU."

Figure 6-10 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 Record 2, because the user matches at least one marking “RD” on the Record 2. Because the user has not been assigned the supplemental marking “AU,” the user still cannot access Record 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 record.

Supplemental markings are *not* inherited by records folders or records. Markings are checked at every folder and record level. Supplemental markings do not have any permissions hierarchy; that is, permissions have a flat hierarchy in that all markings have equal permissions: access granted or access denied to records users. In contrast, the classified security does have a hierarchy to its classification levels. For further information, see Classified Records Security Hierarchy (page 6-16).

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 allows you to view information about supplemental markings.
- **Admin.RecordManager**—In addition to viewing information about supplemental markings, this right also allows 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.

Permissions: Content Server system administrator permissions are required to perform this action.

Managing Supplemental Markings

The following procedures are followed when managing supplemental markings:

- Enabling or Disabling Supplemental Markings (page 6-6)
- Creating or Editing a Supplemental Marking (page 6-7)
- Viewing Supplemental Marking Information and References (page 6-8)
- Deleting a Supplemental Marking (page 6-9)
- Assign or Remove User Supplemental Markings (page 6-9)
- Using Restricted and Formerly Restricted Supplemental Markings (page 6-11)

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 records and records folders.

Disabling supplemental markings means that the security provided by the markings is not in force; however, the supplemental markings can still be used generically as document handling instructions.

Permissions: The Admin.RecordManager right is required to perform these actions. This right is assigned by default to the ‘rmaadmin’ role.

1. Select **Administration—Configure Records Management.**

The Configure Records Management Page (page 7-2) is displayed.

2. Enable the **Supplemental Markings** check box.
3. (Optional) To force a user to match **all** supplemental markings assigned to a record or records folder before granting access, select the **User must match all Supplemental Markings** check box. To allow access if the user has at least one of the markings, leave the box unchecked.
4. Click **Submit**. The configuration successful message is displayed.

To disable supplemental markings, clear the **Supplemental Markings** check box and the **User must match all supplemental markings** check box. Click **Submit**. A configuration successful message is displayed. Supplemental markings are now disabled and the Supplemental Marking selection field is hidden from view.

Creating or Editing a Supplemental Marking

You can create supplemental markings only if they are enabled. See Enabling or Disabling Supplemental Markings (page 6-6) for details.

After you create a supplemental marking, it is available for applying to records, records folders, and users.

When editing an existing supplemental marking, you can modify its description, but not its name.

Permissions: The Admin.RecordManager right is required to perform these actions. This right is assigned by default to the 'rmaadmin' role.

1. Select **Configure—Supplemental Markings** from the Configure Records Management Page (page 7-2).

   The Access Supplemental Markings Page (page 6-11) is displayed.
2. Click **Add**.

   The Create or Edit Supplemental Marking Page (page 6-12) is displayed.
3. Enter a unique supplemental marking of up to 30 characters in the **Supplemental Marking** text box.
4. Enter a description of the marking up to a maximum of 30 characters in the **Brief Description** text box.
5. Click **Create**.

6. The Supplemental Marking Information Page (page 6-13) is displayed with a message indicating the creation was successful. You can use that page to edit or delete the marking, or view references to the marking.
7. Click **OK** when done.

To edit an existing supplemental marking, complete the following steps:

1. Select **Configure—Supplemental Markings** from the Configure Records Management Page (page 7-2).

   The Access Supplemental Markings Page (page 6-11) is displayed.
2. You can edit the marking in one of two ways:
   - Select Edit Marking from the item's Action menu. The Create or Edit Supplemental Marking Page (page 6-12) is displayed.
   - Click on the name of the marking you want to edit. The Supplemental Marking Information Page (page 6-13) is displayed. Click **Edit** on that page. The Create or Edit Supplemental Marking Page (page 6-12) is displayed.
3. Make your changes and click **Submit Update**. The Supplemental Marking Information Page (page 6-13) is displayed with a message indicating the creation was successful. You can use that page to edit or delete the marking, or view references to the marking.
4. Click **OK** when done.

Viewing Supplemental Marking Information and References

Permissions: Either the Admin.Triggers or Admin.RecordManager right is required to perform these actions. The Admin.Triggers right is assigned by default to the 'rmaprivileged' and 'rmaadmin' roles, and the Admin.RecordManager right to the 'rmaadmin' role.

1. Select **Configure—Supplemental Markings** from the Configure Records Management Page (page 7-2).

   The Access Supplemental Markings Page (page 6-11) is displayed.
2. Click the name of the marking with information to view.
3. The Supplemental Marking Information Page (page 6-13) is displayed. You can use that page to edit or delete the marking, or view references to the marking.
4. Click **OK** when done.

Deleting a Supplemental Marking

You can delete supplemental markings regardless of whether markings are enabled. You cannot delete a supplemental marking until you remove any references to the marking in records or records folders. You must also manually remove the supplemental markings assignments from users.

If you attempt to delete a supplemental marking that is currently in use, a message is displayed stating that the marking is in use by users (the marking is assigned to users and must be removed), by records folders, or by a record. You must then remove the supplemental marking(s) from the user, records folder, or records before proceeding.

Permissions: The Admin.RecordManager right is required to perform this action. This right is assigned by default to the ‘rmaadmin’ role.

Tech Tip: 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 records objects have the marking in use. You can also use screening folders to quickly isolate records objects by supplemental markings. For further information, see the *Records Manager DoD Edition System Maintenance Guide.*.

1. Select **Configure—Supplemental Markings** from the Configure Records Management Page (page 7-2).

   The Access Supplemental Markings Page (page 6-11) is displayed.

2. In the Supplemental Marking area, select **Delete** from the item’s Action menu. To delete multiple markings, select the checkbox next to the marking name and click **Delete**. You can also delete a marking when viewing the marking’s Supplemental Marking Information Page (page 6-13).

3. A message indicates deleting the marking was successful.

4. Click **OK**.

Assign or Remove User Supplemental Markings

Permissions: Administrator privileges in Content Server are required to perform this action.

Before assigning markers to users, make sure you have enabled supplemental markings, created the markings, assigned supplemental markings to records folders and records, and assigned roles to the records users. For the most strict supplemental marking security, you can also force a user to pass all supplemental markings to access a record or records 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.

Note: To disable use of supplemental markings as a security feature, do not assign the markings to users.

1. Select **Admin Applets** from the **Administration** tray.
2. Click the **User Admin** icon.

   The User Admin utility starts.
3. On the Users tab, select the user in the Users list, and click **Edit**. The Edit User screen—Info tab is displayed.
4. In the **Supplemental Markings** field, select the markings to which the user should have access. Click the options list arrow, and click the marking you want. You can assign multiple markings to a user.
5. Click **OK**. Repeat the process for each user you need to assign supplemental marking access.
6. Restart the content server.

To remove a supplemental marking from a user, complete the following steps:

1. Select Admin Applets from the **Administration** tray.

   The Administration Applets page for your server is displayed.
2. Click the **User Admin** icon.

   The User Admin utility starts.
3. On the Users tab, select the user in the Users list, and click **Edit**. The Edit User screen**—**Info tab is displayed.
4. In the **Supplemental Markings** field, delete a marking by editing the text in the **Supplemental Markings** text box. Use the delete or backspace key to remove the marking.

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 that has a marking you need to remove.

6. Restart the Content Server. For more information about restarting the Content Server, see the Content Server administration online help or the *Records Manager DoD Edition Installation Guide*.

Using Restricted and Formerly Restricted Supplemental Markings

Restricted Data and *Formerly Restricted Data* are supplemental markings that ship with the product. You can use either of these markings alone or in combination with other markings to disable classified metadata fields on the content check-in and metadata update forms:

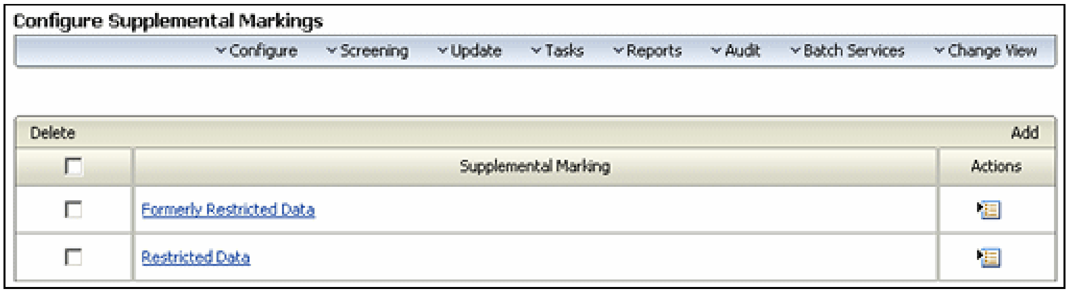
1. Enable supplemental markings (see Enabling or Disabling Supplemental Markings (page 6-6)).
2. Select *Restricted Data* or *Formerly Restricted Data* as the supplemental marking.
3. Restart the content server.

Supplemental Markings Interface

The following screens are used when managing supplemental markings:

- Access Supplemental Markings Page (page 6-11)
- Create or Edit Supplemental Marking Page (page 6-12)
- Supplemental Marking Information Page (page 6-13)

Access Supplemental Markings Page

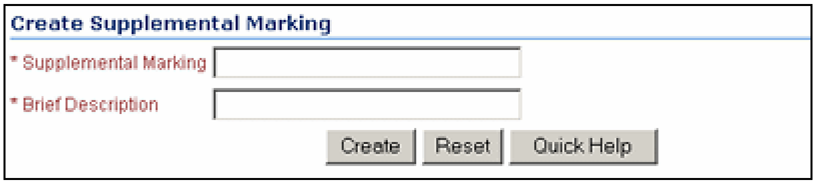


□	Supplemental Marking	Actions
□	Formerly Restricted Data	▤
□	Restricted Data	▤

This page is used to view, delete, or add supplemental markings. It is available when the **Use Supplemental Markings** check box is selected in the Configure Records Management Page (page 7-2).

To access the page, select **Configure—Supplemental Markings** on the Configure Records Management Page (page 7-2). The page menu options are the same as those on the Configure Records Management Page (page 7-2).

Create or Edit Supplemental Marking Page



Create Supplemental Marking

* Supplemental Marking	
* Brief Description	

Permissions: The Admin.RecordManager right is required to use this page. This right is assigned by default to the ‘rmaadmin’ role.

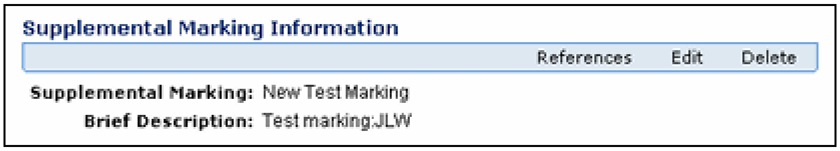
Use the Create page to define a new supplemental marking. To access this page, select **Add** on the Access Supplemental Markings Page (page 6-11).

Use the Edit page to modify the properties of an existing supplemental marking. To access the page, choose Edit from the item’s Action menu. You can also click on the item on the Access Supplemental Markings Page (page 6-11) then select **Edit** from the Supplemental Marking Information Page (page 6-13).

Feature	Description
Supplemental Marking	Enter a unique name or acronym for the supplemental marking. ❖ Required. ❖ Maximum characters: 30. This field is view-only on the edit page.
Brief Description	Enter a brief description of the marking. ❖ Required. ❖ Maximum characters: 30.
Create button (Create page only)	Creates the supplemental marking. The supplemental marking does not appear in the Supplemental Marking list until you assign the marking to yourself. See Assign or Remove User Supplemental Markings (page 6-9).

Feature	Description
Submit Update button (Edit page only)	Submits your updated edits to the description.
Reset button	If you are creating a new supplemental marking, this resets the page to its initial default settings. If you are editing an existing supplemental marking, this returns your original settings.

Supplemental Marking Information Page


Supplemental Marking Information

Supplemental Marking: New Test Marking
Brief Description: Test marking:JLW

Permissions: Either the Admin.Triggers or Admin.RecordManager right is required to use this page. The Admin.Triggers right is assigned by default to the ‘rmaprivileged’ and ‘rmaadmin’ roles, and the Admin.RecordManager right to the ‘rmaadmin’ role. With the Admin.Triggers right, you can only view information about supplemental markings. With the Admin.RecordManager right, you can also add, edit, and delete supplemental markings.

This page is used to view information about a marking. To access this page, select a marking on the Access Supplemental Markings Page (page 6-11). You can also use this page to delete the marking, edit the marking, or view the references to the marking.

SECURITY CLASSIFICATIONS

Note: Classifications are available for records only. They are not used with non-record content.

The classification of records is the process of identifying and safeguarding records that require protection against unauthorized disclosure—for example, because they contain information sensitive to the national security of the United States. Records classification can be an additional way to restrict records access in conjunction with supplemental markings and custom security fields. Classification markings are at the record level only, unlike supplemental markings, which are at the record or record folder level.

This section discusses the following topics:

- About Records Classification (page 6-14)
- Managing Classified Security (page 6-16)
- Classification Interface (page 6-24)

About Records Classification

DoD Edition offers a number of features specifically geared to handling and processing classified records in accordance with the Chapter 4 requirements of the DoD 5015.2 specification. You need to enable this functionality before you can use it (see Enabling or Disabling Classified Security (page 6-17)).

A record is marked as a classified record using a classification that specifies the security level of the record. A number of built-in records classifications ("Top Secret," "Secret," and "Confidential") are available, but you can also create your own custom classifications (see Creating or Editing a Security Classification (page 6-18)).

Records are either classified, unclassified, or declassified:

- **Classified records** have an initial classification and a current classification. The classification when a record is initially filed is tracked, and the current classification of the record is as well. A record has an initial classification (specified when it is first filed) and a current classification, which may be different from the initial classification. All changes to record classification are tracked in the audit logs in the Record History reports.
- **Unclassified records** are any records that are not and have never been classified. The majority of records in a records database are most likely unrestricted, depending on the database of the agency.
- **Declassified records** are any records that were formerly classified. When a record is filed and classified, it typically must be declassified within a ten year period. Any exceptions to this must be given an exemption category. When a declassify date

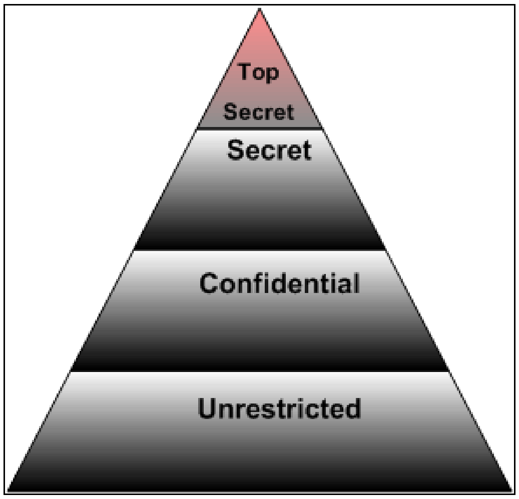
exceeds the ten year period after the publication (filing) date, an alert reminds the user to enter an exemption category for the record.

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 (that is, unclassified)

Figure 6-11 Classified records hierarchy



Top Secret

According to EO (Executive Order) 12958, the Top Secret classification level 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.”

Only the President of the United States has the authority to classify a record as Top Secret, pursuant to the Executive Order 12958. For further details, access the following link: http://www.fas.org/sgp/clinton/eo12958.html

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.”

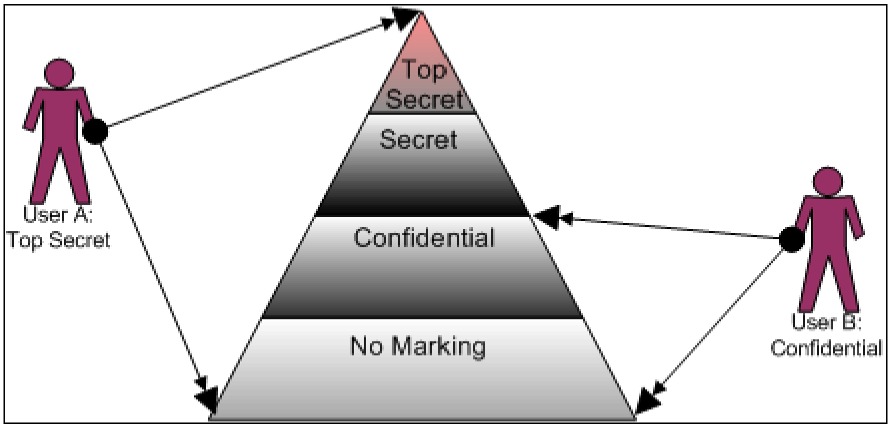
Confidential

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.”

Classified Records Security Hierarchy

Every records user has access to unclassified records, provided all other security criteria are met, such as supplemental markings. A user who has access to Top Secret classification has access to all lower classifications as well, as shown for User A in the figure below. User B has access to Confidential records and unclassified records.

Figure 6-12 Hierarchical user access



Managing Classified Security

The following tasks are included in managing classifications:

- Enabling or Disabling Classified Security (page 6-17)
- Creating or Editing a Security Classification (page 6-18)
- Setting the Order of Security Classifications (page 6-19)
- Deleting a Security Classification (page 6-20)

- Setting the Declassification Time Frame (page 6-20)
- Assigning a Classification to a User (page 6-22)
- Changing a User's Classification (page 6-23)
- Removing a User's Classification (page 6-23)

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 records.

After you enable classified security, you can create any custom security classifications required by your organization. If you create any additional security classifications, make sure you indicate its place within the marking hierarchy. For further information, see Setting the Order of Security Classifications (page 6-19).

Permissions: The Admin.RecordManager right is required to perform this action. This right is assigned by default to the 'rmaadmin' role.

1. Select **Configure Records Management** from the **Administration** tray.

   The Configure Records Management Page (page 7-2) is displayed.

2. Enable the **Classified Security** check box.
3. Click **Submit**. A message is displayed stating that the configuration was updated successfully.

To disable classified security, complete the following steps:

Caution: Disabling classified security puts sensitive classified records at risk of being accessed by unauthorized people. After your classified security is in force, it is not recommended that you disable it.

1. Select **Configure Records Management** from the **Administration** tray.

   The Configure Records Management Page (page 7-2) is displayed.

2. Clear the **Classified Security** check box.
3. Click **Submit**. A message is displayed stating that 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.

Creating or Editing a Security Classification

Use this procedure to create a new security classification. After you create a custom classification, you must indicate its order in the hierarchy. If you do not, the security classification is ignored. For further information, see Setting the Order of Security Classifications (page 6-19).

You can create security classifications only if the classified security feature has been enabled (see Enabling or Disabling Classified Security (page 6-17)).

When editing an existing security classification, you can modify its description, but not its name.

Permissions: The Admin.RecordManager *and* Admin.SecurityClassifications rights are required to perform these actions. These rights are assigned by default to the 'rmaadmin' role.

1. Select **Configure—Classification—Security Classification** from the Configure Records Management Page (page 7-2) page.

   The Configure Security Classification Page (page 6-24) is displayed.

2. Click **Add**.

   The Create or Edit Security Classification Page (page 6-25) is displayed.

3. Enter a unique classification of up to 30 characters in the **Security Classification** text box.

4. Enter a description up to a maximum of 30 characters in the **Brief Description** text box.

5. Click **Create**. A message indicates creating the classification was successful.

6. Click **OK**. The Configure Security Classification Page (page 6-24)is displayed with the new classification in the list. You must be assigned the classification level or a higher level to be able to view the security classification level. You must indicate the placement of the new classification in the hierarchy. For further information, see Setting the Order of Security Classifications (page 6-19).

Permissions: When editing a classification, you must also be assigned the highest security level to view all of the available classifications for editing.

To edit an existing security classification, complete the following steps:

1. Select **Configure—Classification—Security Classification** from the Configure Records Management Page (page 7-2) page.

The Configure Security Classification Page (page 6-24)is displayed.

2. Select the classification to edit and click **Info**.

   The Security Classification Information Page (page 6-26) is displayed.

3. Click **Edit**.

   The Create or Edit Security Classification Page (page 6-25) is displayed.

4. Make your changes in the **Brief Description** text box, and click **Submit Update**. A message is displayed stating that the security classification was updated successfully.

5. Click **OK**.

Setting the Order of Security Classifications

Prerequisites:

- Create any custom security classifications required for your organization. See Creating or Editing a Security Classification (page 6-18).
- Assign yourself the highest classification level so that you can view and reorder all levels. See Changing a User's Classification (page 6-23).

Permissions: The Admin.RecordManager *and* Admin.SecurityClassifications rights are required to perform this action. These rights are assigned by default to the 'rmaadmin' role. You must also have the 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 you only use the built-in security classifications in their default order, this procedure is not needed.

1. Select **Configure—Classification—Security Classification** from the Configure Records Management Page (page 7-2) page.

   The Configure Security Classification Page (page 6-24)is displayed.

2. Use the up arrow (⬆) and down arrow (⬇) to move a selected security classification up or down in the classification hierarchy. The highest classification should be at the top of the list, and the lowest at the bottom.

Important: The last item in the list will be unclassified regardless of the name that you assign to it. Make sure that you have a "classification" in your hierarchy that you intend to be unclassified.

3. Click **Submit Update**. A message is displayed stating that the configuration was updated successfully.

Deleting a Security Classification

You cannot delete a classification until you remove any references to that classification in records (see Viewing Security Classification References (page 6-21)). You must also manually remove the security classification assignments from users (see Removing a User’s Classification (page 6-23)). If you attempt to delete a security classification that is still in use, a message is displayed stating that the classification is in use by users (it is assigned to users and must be removed) or by a record.

Tech Tip: You can search for security classifications from the Search page. Use the search results to see which records have the classification in use. You can also use screening to quickly isolate records. For further information, see the *Records Manager DoD Edition System Maintenance Guide*.

Permissions: The Admin.RecordManager *and* Admin.SecurityClassifications rights are required to perform this action. These rights are assigned by default to the ‘rmaadmin’ role. You must also be assigned the highest security level to view all of the available classifications for deleting.

1. Select **Configure—Classification—Security Classification** from the Configure Records Management Page (page 7-2) page.

   The Configure Security Classification Page (page 6-24)is displayed.

2. Select the security classification to delete, and click **Info**.

   The Security Classification Information Page (page 6-26) is displayed.

3. Click Delete from the Page menu. A message is displayed stating that the security classification was deleted successfully.

4. Click **OK**.

Setting the Declassification Time Frame

The default declassification retention period for records is ten years. This means records are automatically declassified after ten years unless they were exempted from declassification. When a record 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.

Permissions: The Admin.PrivilegedEnvironment right is required to perform this action. This right is assigned by default to the ‘rmaprivileged’ and ‘rmaadmin’ roles.

1. Select **Administration—Configure Records Management**.
2. The Configure Records Management Page (page 7-2) is displayed.
3. In the “Maximum years before declassifying” field, enter the number of years after which records will be declassified (the default is 10). If you do not see this field, you probably do not have the Admin.PrivilegedEnvironment right.
4. Click **Submit Update**. A message is displayed stating that records management has been configured successfully.
5. Click **OK**.

Viewing Security Classification References

Use this procedure to view references to a security classification—those disposition rules which use the security classification in their definitions.

Permissions: The Admin.RecordManager *and* Admin.SecurityClassifications rights are required to perform this action. These rights are assigned by default to the ‘rmaadmin’ role. You must also be assigned the highest security level to view all of the available classifications for viewing.

1. Select **Configure—Classification—Security Classification** from the Configure Records Management Page (page 7-2) page.

   The Configure Security Classification Page (page 6-24)is displayed.
2. Select the security classification to view, and click the **Info** icon.

   The Security Classification Information Page (page 6-26) is displayed.
3. Select **Reference** from the Page menu.

   The Security Classification References Page (page 6-27) is displayed

   This page shows all users and content items that are assigned the selected security classification level. If you click any of the content links, the associated content information page for that item is displayed.

Assigning a Classification to a User

You can assign security classifications only if the classified security feature has been enabled (see Enabling or Disabling Classified Security (page 6-17)).

Permissions: Administrator privileges in Content Server (‘sysadmin’ permissions) are required to assign user access to classifications. Your own assigned classification level must also be at least the level that is 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. Select **Admin Applets** from the **Administration** tray.

   The Administration Applets page for your server is displayed.

2. Click the **User Admin** icon.

   The User Admin utility starts.

3. On the Users tab, select the user in the Users list, and click **Edit**. The Edit User screen is displayed.

4. Make sure the Info tab is active.

5. In the **Security Classification** field, select the maximum security level that the user should have access to from the option list available on the pull-down menu.

6. Click **OK**. Repeat the process for each user.

Note the following considerations:

- If you do not assign any security classification to a user, that user will not be able to pick an initial classification while checking in a record. Because specifying the initial classification is mandatory, this means the user can then not check the record into the content server.

- It is recommended that you assign the highest security classification to the records manager and system administrator. This allows them to perform all classification-related tasks on records (for example, on behalf of someone who needs to downgrade or declassify a record, but does not have the required classification privileges).

Changing a User's Classification

The assigned security classification of users determines what records they can access.

Permissions: Administrator privileges in Content Server ('sysadmin' permissions) are required to perform this action. Your own assigned classification level must also be at least the level that is being accessed.

1. Select **Admin Applets** from the **Administration** tray.

   The Administration Applets page for your server is displayed.

2. Click the **User Admin** icon.

   The User Admin utility starts.

3. On the Users tab, select the user in the Users list, and click **Edit**. The Edit User screen is displayed.
4. Make sure the Info tab is active.
5. In the **Security Classification** field, select the new maximum security level that the user should have access to. Click the options list arrow, and click the classification you want.
6. Click **OK**.
7. Restart the content server. For more information about the methods of restarting the server, see the Content Server administration online help or the *Records Manager DoD Edition Installation Guide*.

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. You must remove any references to a classification before you can delete it.

Permissions: Administrator privileges in Content Server ('sysadmin' permissions) are required to perform this action. Your own assigned classification level must also be at least the level that is being accessed.

1. Select **Admin Applets** from the **Administration** tray.

   The Administration Applets page for your server is displayed.

2. Click the **User Admin** icon.

   The User Admin utility starts.

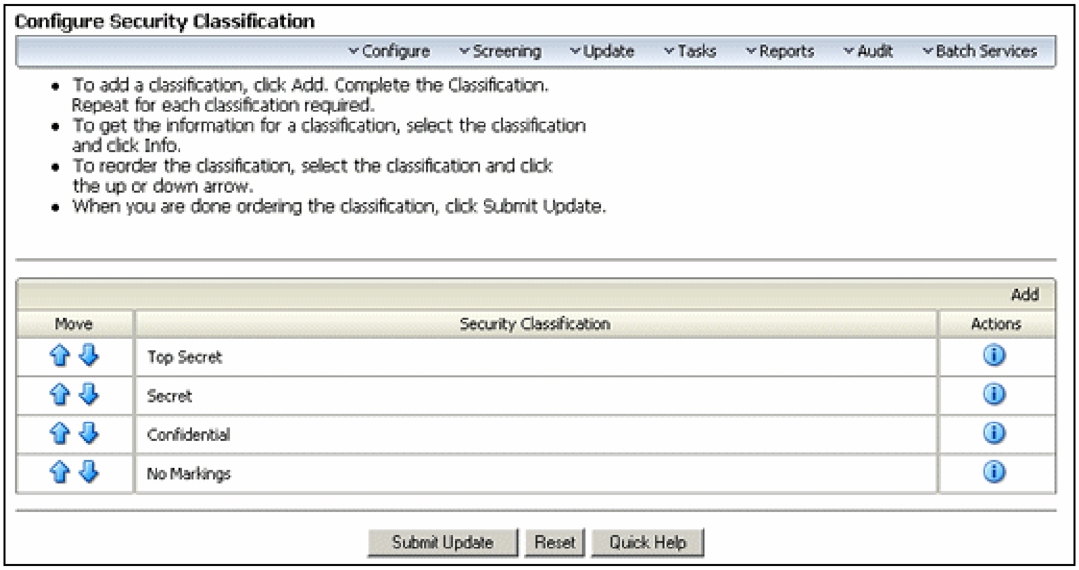
3. On the Users tab, select the user in the Users list, and click **Edit**. The Edit User screen is displayed.
4. Make sure the Info tab is active.
5. In the **Security Classification** field, delete the current security level (using the keyboard or by selecting the blank line from dropdown list).
6. Click **OK**.
7. Restart the content server. For more information about the methods of restarting the server, see the Content Server administration online help or the *Records Manager DoD Edition Installation Guide*.

Classification Interface

The following screens are used to manage classifications:

- Configure Security Classification Page (page 6-24)
- Create or Edit Security Classification Page (page 6-25)
- Security Classification Information Page (page 6-26)
- Security Classification References Page (page 6-27)

Configure Security Classification Page



- To add a classification, click Add. Complete the Classification. Repeat for each classification required.
- To get the information for a classification, select the classification and click Info.
- To reorder the classification, select the classification and click the up or down arrow.
- When you are done ordering the classification, click Submit Update.

Add

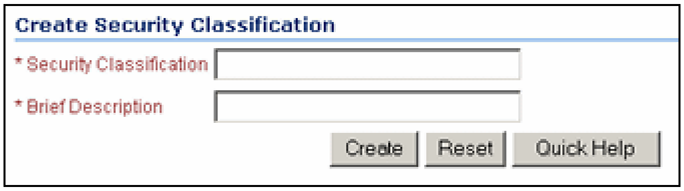
Move	Security Classification	Actions
⇧ ⇩	Top Secret	ⓘ
⇧ ⇩	Secret	ⓘ
⇧ ⇩	Confidential	ⓘ
⇧ ⇩	No Markings	ⓘ

Permissions: The Admin.RecordManager *and* Admin.SecurityClassifications rights are required to use this page. These rights are assigned by default to the ‘rmaadmin’ role.

Use this page to create security classifications and set the classification hierarchy. To access this page, select **Configure—Security Classification** from the Configure Records Management Page (page 7-2) page.

Feature	Description
Up arrow (⬆) Down arrow (⬇	Moves a selected security classification upward or downward one step in the hierarchy with each click.
Add button	Displays the Create or Edit Security Classification Page (page 6-25), where you can define a security classification.
Info button	Displays the Security Classification Information Page (page 6-26), where you can view information and references for the selected security classification. If you have the appropriate rights, you can also edit or delete the security classification using the Actions list on the Security Classification page.
Submit Update button	Submits the updated configuration.

Create or Edit Security Classification Page



Create Security Classification

* Security Classification	
* Brief Description	

Permissions: The Admin.RecordManager *and* Admin.SecurityClassifications rights are required to use this page. These rights are assigned by default to the ‘rmaadmin’ role.

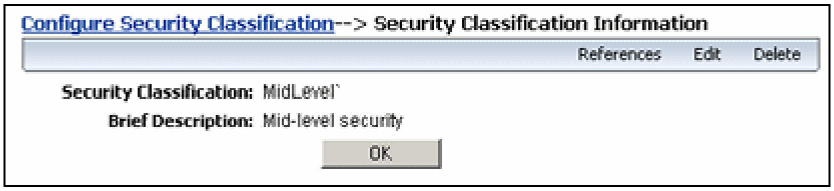
Use the Create page to define a security classification. After you create a classification, be sure to indicate its order among the other available security classifications, both built-in and custom. For further information, see Setting the Order of Security Classifications (page 6-19). You must have permissions to that level to view it.

To access the Create page, click **Add** on the Configure Security Classification Page (page 6-24).

Use the Edit page to modify the properties of an existing security classification. To access this page, select a classification from the list on the Configure Security Classification Page (page 6-24)and click **Info**. From the **Actions** list, click **Edit**.

Feature	**Description**
Security Classification	A unique name or acronym for the security classification. ❖ Required. ❖ Maximum characters: 30. This field is view-only on the edit page.
Brief Description	A brief description of the security classification. ❖ Required. ❖ Maximum characters: 30.
Create button (Create page only)	Creates the security classification.
Submit Update button (Edit page only)	Submits your updates to the description.
Reset button	If you are creating a new security classification, this resets the page to its initial default settings. If you are editing an existing security classification, this returns your original settings.

Security Classification Information Page


Configure Security Classification--> Security Classification Information
References
Edit
Delete
OK

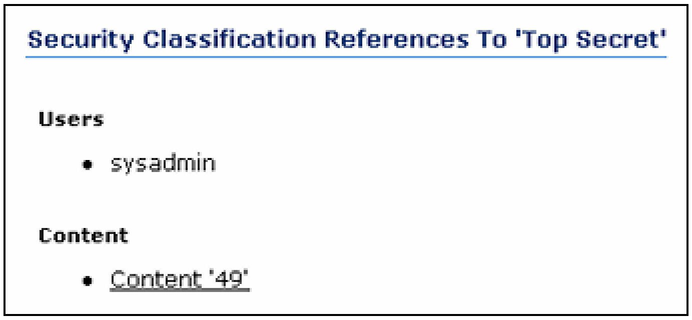
Security Classification: MidLevel`

Brief Description: Mid-level security

Permissions: The Admin.RecordManager *and* Admin.SecurityClassifications rights are required to use this page. These rights are assigned by default to the 'rmaadmin' role. You must also have the security classification level assigned to you to view or work with it.

To access this page, select a classification on the Configure Security Classification Page (page 6-24)and click **Info**.

Security Classification References Page



Security Classification References To 'Top Secret'

Users

- sysadmin

Content

- Content '49'

Permissions: The Admin.RecordManager *and* Admin.SecurityClassifications rights are required to use this page. These rights are assigned by default to the ‘rmaadmin’ role. You must also have the security classification level assigned to you to view or work with it.

To access this page, select a classification on the Configure Security Classification Page (page 6-24)and click **Info**. Select **References** from the **Actions** menu.

CUSTOM SECURITY FIELDS

Note: Custom security fields are available for records only. They are not available for non-record content.

Custom security fields—or custom supplemental markings as they are called in the DoD 5015 standard—are optional, and are another layer of security in addition to supplemental markings (see Supplemental Markings (page 6-3)).

Custom security fields are really just a customized version of supplemental markings, except that with custom security fields, you can configure any custom field (except date fields) to be matched by a user rather than a designated supplemental marking. Unlike supplemental markings, custom security fields are enforced only at the record level. Supplemental markings are enforced at both the records folder and the record level.

This section covers the following topics:

❖ About Custom Security Fields (page 6-28)

- Managing Custom Security (page 6-28)
- Custom Security Field Example (page 6-31)
- Custom Security Interface (page 6-35)

About Custom Security Fields

A 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 a record assigned with custom security. If the “match all” setting is enabled, then a user must be assigned to all the same projects as a record is assigned to in order to access the record with multiple project assignments. If a user does not match all project names, the user cannot access a record.

You add the document (record) information version of the custom security field in Content Server’s Configuration Manager utility, and then add a mirror image of the custom security field to the User Admin utility. The options list for the custom security fields are populated with identical multiple project names. You also use the User Admin utility to assign users to the custom security field list options. In DoD Edition, you create the custom security field that points the document and user fields to each other.

You can opt to select the “match all” feature for custom security fields just as you can with supplemental markings. Record or document 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 a record is checked in with multiple field options assigned (for example, “Pangea” and “Tectonic”), then only a user with all project names assigned (i.e., user2) can access that record. If the “match all” setting is disabled, then a user only needs to match one field option to access a record.

To work with custom security fields, you need to have one of the following rights:

- **Admin.Triggers**—This right allows you to view information about custom security fields.
- **Admin.RecordManager—**In addition to viewing information about custom security fields, this right also allows you to create (add), edit, and delete custom security fields.

Managing Custom Security

The following tasks are often performed when managing custom security:

- Enabling or Disabling Custom Security Field Usage (page 6-29)

- Creating or Editing a Custom Security Field (page 6-29)
- Viewing Custom Security Field Information (page 6-31)
- Deleting a Custom Security Field (page 6-31)

Enabling or Disabling Custom Security Field Usage

Use this procedure to enable the custom security field feature. You can enable and disable custom security fields at any time.

Permissions: The Admin.RecordManager right is required to enable custom security fields. This right is assigned by default to the ‘rmaadmin’ role.

1. Select **Configure Records Management** from the **Administration** tray.

   The Configure Records Management Page (page 7-2) is displayed.
2. Select the **Custom Security Fields** check box.
3. Click **Submit Update**. A message is displayed saying that records management has been configured successfully.
4. Click **OK**.

Use this procedure to disable the custom security field feature. When you disable the custom security field feature, the custom security fields are not enforced.

1. Select **Configure Records Management** from the **Administration** tray.

   The Configure Records Management Page (page 7-2) is displayed.
2. Clear the **Custom Security Fields** check box.
3. Click **Submit Update**. A message is displayed saying that records management has been configured successfully.

Creating or Editing a Custom Security Field

Use this procedure to create a new custom security field. Make sure that you have defined the custom field for the documents (records) in Content Server’s Configuration Manager utility, as well as the custom field for the users in Content Server’s User Admin utility. See Custom Security Field Example (page 6-31) for step-by-step instructions for setting up a custom security field.

Note: You can create custom security fields only if the custom security field feature has been enabled (see Enabling or Disabling Custom Security Field Usage (page 6-29)).

Permissions: The Admin.RecordManager right is required to perform this action. This right is assigned by default to the predefined ‘rmaadmin’ role.

1. Select **Configure—Custom Security Fields**from the Configure Records Management Page (page 7-2).

   The Configure Custom Security Field Page (page 6-35) is displayed.

2. In the Custom Security Field area, click **Add**.

   The Create or Edit Custom Security Field Page (page 6-35) is displayed.

3. Enter a name for the field in the **Custom Security Field** text box.
4. Select the document metadata name for the content field from the **Content Field** list.
5. Select the metadata name of the user field from the **User Field** list.
6. (Optional) Select the **Match all** check box to force the user entries to match **all** content field entries. Leave this check box cleared to allow only one content field to match the user field.
7. Click **Create**. The successfully created custom security field message is displayed.
8. Click **OK**.

To edit an existing custom security field, complete the following steps:

1. Select **Configure—Custom Security Fields** from the Configure Records Management Page (page 7-2).

   The Configure Custom Security Field Page (page 6-35) is displayed.

2. Select **Edit Field** from the field’s **Actions** menu.
3. Make your edits:
   a. Select the name of the document metadata field from the **Content Field** list.
   b. Select the name of the user metadata field in the **User Field** list.
   c. Select or clear the **Match all** check box.
4. Click **Submit Update**. A message indicates the update was successful.
5. Click **OK**.

Viewing Custom Security Field Information

Permissions: Either the Admin.Triggers or Admin.RecordManager right is required to perform this action. The Admin.Triggers right is assigned by default to the ‘rmaprivileged’ and ‘rmaadmin’ roles, and the Admin.RecordManager right to the ‘rmaadmin’ role.

1. Select **Configure—Custom Security Fields** from the Configure Records Management Page (page 7-2).

   The Configure Custom Security Field Page (page 6-35) is displayed.

2. In the custom field area, click on the field to view.

   The Custom Security Field Information Page (page 6-37) is displayed.

3. Click **OK** when done.

Deleting a Custom Security Field

You can delete a custom security field without having to remove references to it by users and records, unlike supplemental markings and security classifications.

Permissions: The Admin.RecordManager right is required to delete a custom security field. This right is assigned by default to the ‘rmaadmin’ role.

1. Select **Configure—Custom Security Fields** from the Configure Records Management Page (page 7-2).

   The Configure Custom Security Field Page (page 6-35) is displayed.

2. Select **Delete** from the item’s **Actions** menu. To delete multiple fields, select the checkbox next to the field name and click **Delete**. You can also delete a field when viewing the field’s Custom Security Field Information Page (page 6-37).
3. A message displays, indicating the deletion was successful.
4. Click **OK**.

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 (page 6-32). The name must be the same as the custom security field.

2. Create the Custom Security Field in User Admin (page 6-33). The field name must be the same. The content server assigns the “u” prefix. Assign the field options to the user.
3. Rebuild the content server search index, and restart the server. Complete instructions are in the *DoD Edition Installation Guide*.
4. Create the Custom Security Field in DoD Edition (page 6-34) using the exact field names defined in the Content Server’s utilities.

After the custom security field is set up, you can test the field by checking in and accessing records assigned field options. See Verify the Custom Security Field (page 6-34).

Create the Custom Security Field in Configuration Manager

This portion of the example creates the custom security field as a document (record) field within Content Server’s Configuration Manager utility. The field will be available for use on the document or record check-in form.

1. Select **Admin Applets** from the **Administration** tray on the left.

   The Administration Applets page for your server is displayed.
2. Click the **Configuration Manager** icon.

   The Configuration Manager utility starts.
3. Click the **Information Fields** tab.
4. Click **Add**.

   The Add Custom Info Field screen is displayed.
5. Type `ProjectName`, and click **OK**. The Add Custom Info Field screen is displayed. Specify the field attributes:
   a. In the **Field Caption** text box, enter a space between any compound words (that is, “Project” and “Name”) so that your field label displays properly.
   b. In the **Field Type** list, select **Long Text**.
   c. Select the **Enable Options List** check box. The Configure button becomes enabled. Click this button.
   d. The Configure Option List screen opens. In the **Options List Type**, select the **Edit and Multiselect List** option.
   e. Click **Edit** next to **Use Option List**. The Option List screen is displayed.

   f. In the options list, type `Pangea`. Press Enter for a carriage return, and then type `Tectonic`. Click **OK** three times.

6. Click **Update Database Design**.

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 Content Server’s User Admin utility. It also assigns project names to the user named “user1,” which is an out-of-the-box test user that ships with content server. The options list you create here must match exactly the options list you created in Configuration Manager.

1. Select **Admin Applets** from the **Administration** tray.

   The Administration Applets page for your server is displayed.

2. Click the **User Admin** icon.

   The User Admin utility starts.

3. Open the **Information Fields** tab.

4. Click **Add**.

   The Add Custom Info Field screen is displayed.

5. Type `ProjectName`, and click **OK**. The Add Metadata Field screen is displayed. Specify the field attributes:

   a. In the **Field Caption** text box, enter a space between any compound words (that is, “Project” and “Name”) so that your field label displays properly.

   b. In the **Field Type** list, select **Long Text**.

   c. Select the **Enable Options List** check box. The Options List Settings tab becomes enabled.

   d. In the **Options List Type**, select the **Edit and Multiselect List** option.

   e. Click **Edit**. The Option List screen is displayed.

   f. In the options list, type `Pangea`. Press Enter for a carriage return, and then type `Tectonic`. Click **OK** twice.

6. Click **Update Database Design**.

7. Click the **Users** tab. In the User Name list, select “user1”, and click **Edit**. The Edit User “user1” screen is displayed.
   a. In the Project Name dropdown list, click the down arrow, and click the project name “Pangea” from the list. Repeat for “Tectonic.” Note that you now have a comma-separated list of project names assigned to user1.
   b. Click **OK**.
8. Restart the content server.

Create the Custom Security Field in DoD Edition

This portion of the example creates the custom security field within DoD Edition. Make sure the Custom Security Field option is enabled in the Configure Records Management Page (page 7-2), and you have defined the document and user fields in the appropriate administration utilities of Stellent Content Server.

1. Select **Configure—Custom Security Fields** from the Configure Records Management Page (page 7-2).
2. On the Configure Custom Security Field Page (page 6-35), click **Add**.

   The Create or Edit Custom Security Field Page (page 6-35)is displayed.
3. In the **Custom Security Field** text box, type `Project Name`.
4. From the **Content Field** list, select **ProjectName**.
5. From the **User Field** list, select **ProjectName**.
6. Select the **Match all** check box 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 a record, the user cannot access that record.
7. Click **Create**.

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 a record with both “Pangea” and “Tectonic” selected as project names in the check-in form. Search for the record you just checked in as *user1*. The search should be successful.

❖ Log in as a new user without any custom field assignments. Attempt to access the record user1 just checked in. The attempt to view the record should not be successful because the new user does not have any assigned field options.

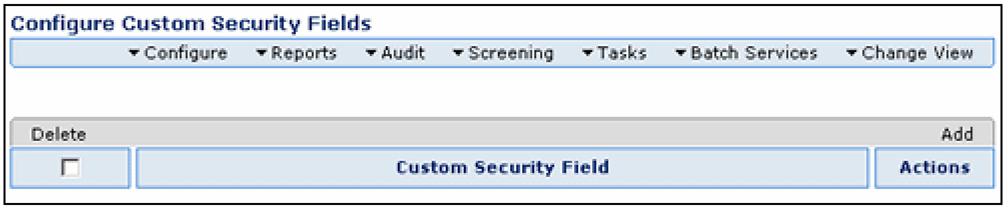
- Log in as an administrator and assign the new user the field option “Pangea.” Disable the **Match all** option for the custom security field. Log in as the new user and attempt to access the record with “Pangea” and “Tectonic” assigned as the project name. The access should now be successful because only one field list option has to match, and the user is assigned the appropriate field list option.

Custom Security Interface

The following screens are used in managing custom security fields:

- Configure Custom Security Field Page (page 6-35)
- Create or Edit Custom Security Field Page (page 6-35)
- Custom Security Field Information Page (page 6-37)

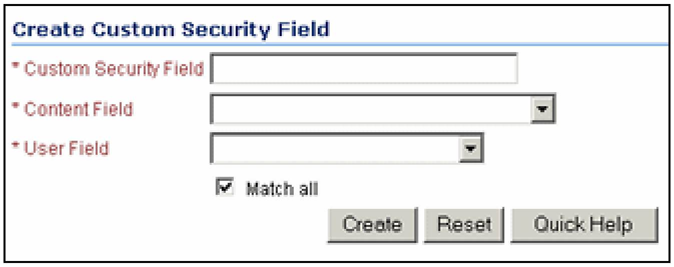
Configure Custom Security Field Page



Configure Custom Security Fields

This page is used to view, delete, or add custom security fields. To access this page, select **Configure—Custom Security Fields** from the Configure Records Management Page (page 7-2).

Create or Edit Custom Security Field Page



Create Custom Security Field

* Custom Security Field
* Content Field
* User Field

☑ Match all

Permissions: The Admin.RecordManager right is required to use this page. This right is assigned by default to the ‘rmaadmin’ role.

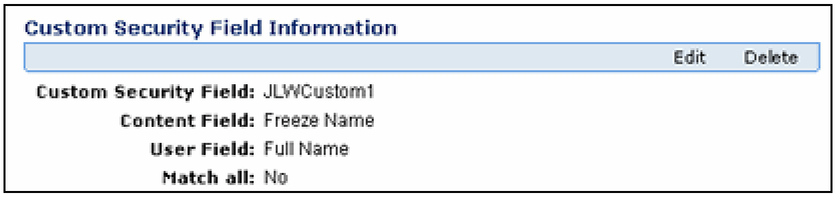
Use the Create page to define a new custom security field. This page is available when the **Custom Security Fields** check box is selected on the Configure Records Management Page (page 7-2). To access the page, click **Add** on the Configure Custom Security Field Page (page 6-35).

Use the Edit page to modify the properties of an existing custom security field. To access this page, choose **Edit** from the item's Action menu on the Configure Custom Security Field Page (page 6-35). You can also click the item on the Configure Custom Security Field Page (page 6-35) then select **Edit** from the Custom Security Field Information Page (page 6-37).

Feature	**Description**
Custom Security Field	A unique name for the custom security field. For example, "Project Name." ❖ Required. ❖ Maximum characters: 30. This field is view-only on the edit page.
Content Field list	Select the content field to match against the user field. The list displays all available content fields, custom or otherwise. ❖ Required. This field must be set up in Content Server's Configuration Manager utility. For an example, see Custom Security Field Example (page 6-31).
User Field list	Select the user field to match against the content field. ❖ Required. This field must also be set up in Content Server's User Admin utility. For an example, see Custom Security Field Example (page 6-31).
"Match all" check box	Select this check box to force the user to match all content field entries to match. Clear this check box to allow access when a user matches at least one content field option. ❖ Optional.

Feature	Description
Create button (Create page only)	Creates the custom security field.
Submit Update button (Edit page only)	Submits your updated edits to the description.
Reset button	If you are creating a new custom security field, this resets the page to its initial default settings. If you are editing an existing custom security field, this returns your original settings.

Custom Security Field Information Page



Custom Security Field: JLWCustom1
Content Field: Freeze Name
User Field: Full Name
Match all: No

Permissions: Either the Admin.Triggers or Admin.RecordManager right is required to use this page. The Admin.Triggers right is assigned by default to the ‘rmaprivileged’ and ‘rmaadmin’ roles, and the Admin.RecordManager right to the ‘rmaadmin’ role. With the Admin.Triggers right, you can only view information about custom security fields. With the Admin.RecordManager right, you can also add, edit, and delete custom security fields. You must also have the security classification level assigned to you to be able to view or work with it.

Use the Custom Security Field Information page to view information about an existing custom security field. To access this page, select a custom field on the Configure Custom Security Field Page (page 6-35). You can also use this page to edit a custom field or delete a custom field.

Classification Guides

Note: Classification guides are for record content only. They can not used with non-record content items.

Classification guides are used to facilitate the proper and uniform derivative classification of information. Specifically, Executive Order 12958 defines “derivative classification” as incorporating, paraphrasing, restating or generating in new form information that is already classified, and marking the newly developed material consistent with the classification markings that apply to the source information.

This section covers the following topics:

- About Classification Guides (page 6-38)
- Managing Classification Guides (page 6-39)
- Classification Guide Interface (page 6-44)

Note: Classification guides can be set up only if the ClassifiedEnhancements component is installed and enabled (see the *Records Manager DoD Edition Installation Guide*).

About Classification Guides

Classification guides (and their associated topics) enable convenient implementation of multiple classification schemes.

They are used to define default values for the following classification-related metadata fields on the content check-in page:

❖ **Initial Classification**	(xInitialClassification)
❖ **Reason(s) for classification**	(xClassificationReason)
❖ **Declassify exemption category**	(xDeclassifyExemptionCategory)
❖ **Declassify on event**	(xDeclassifyOnEventDescription)
❖ **Declassify on date**	(xDeclassifyOnDate)

This makes checking in classified records easier and more consistent, with similar records having the same classification metadata. The records administrator can define multiple classification guides. Each classification guide consists of one or more topics, which provide a further level of detail for grouping classified records.

Note: The default metadata field values associated with a classification topic are suggestions only; they can be overridden, if desired.

Note: Classification guides can be set up only if the ClassifiedEnhancements component is installed and enabled (see the *Records Manager DoD Edition Installation Guide*).

Managing Classification Guides

The following tasks are performed when managing classification guides:

- Creating or Editing a Classification Guide (page 6-39)
- Deleting a Classification Guide (page 6-40)
- Viewing Classification Guide Information (page 6-40)
- Creating or Editing a Classification Topic (page 6-41)
- Editing Classification Topic Settings (page 6-42)
- Deleting a Classification Topic (page 6-43)

Creating or Editing a Classification Guide

Permissions: The Admin.ClassificationGuide right is required to perform this action. This right is assigned by default to the ‘rmaprivileged’ and ‘rmaadmin’ roles.

1. Select **Configure—Classification—Configure Classification Guide** from the Configure Records Management Page (page 7-2).

   The Configure Classification Guide Page (page 6-44) is displayed.

2. Click **Add**.

   The Create or Edit Classification Guide Page (page 6-45) is displayed.

3. Provide a guide ID and a guide name (description), and click **Create**.

   A “Successfully created classification guide” screen is displayed showing the identifier and name of the newly created classification guide. The screen also includes an **Actions** dropdown menu, where you can edit or delete the current classification guide, or add topics to it. See Creating or Editing a Classification Topic (page 6-41).

4. Click **OK** to return to the Configure Classification Guide Page (page 6-44)).

Use this procedure to edit a classification guide:

1. Select **Configure—Classification—Configure Classification Guide** from the Configure Records Management Page (page 7-2).

   The Configure Classification Guide Page (page 6-44) is displayed.

2. In the dropdown list, select the classification guide to edit, and click **Info**.

   The Classification Guide Information Page (page 6-46) is displayed.

3. Select **Edit—Edit Classification Guide** from the Page menu.

   The Create or Edit Classification Guide Page (page 6-45) is displayed.

4. Change the classification guide name as required. You cannot modify the guide ID. Click **Submit Update** when you finish.

   A “Successfully updated classification guide” screen is displayed showing the identifier and modified name of the classification guide. The screen also includes a menu where you can edit or delete the current classification guide, or add topics to it. See Creating or Editing a Classification Topic (page 6-41).

5. Click **OK** to return to the Configure Classification Guide page.

Deleting a Classification Guide

Permissions: The Admin.ClassificationGuide right is required to perform this action. This right is assigned by default to the ‘rmaprivileged’ and ‘rmaadmin’ roles.

1. Select **Configure—Classification—Configure Classification Guide** from the Configure Records Management Page (page 7-2).

   The Configure Classification Guide Page (page 6-44) is displayed.

2. Select the classification guide to delete from the pulldown menu, and click **Delete**.

   The classification guide is deleted.

3. Click **OK** to return to the Configure Classification Guide Page (page 6-44).

Viewing Classification Guide Information

Permissions: The Admin.ClassificationGuide right is required to perform this action. This right is assigned by default to the ‘rmaprivileged’ and ‘rmaadmin’ roles.

1. Select **Configure—Classification—Configure Classification Guide** from the Configure Records Management Page (page 7-2).

   The Configure Classification Guide Page (page 6-44) is displayed.

2. Select the classification guide whose information to view from the pulldown menu, and click **Info**.

   The Classification Guide Information Page (page 6-46) is displayed.

The screen shows the identifier and name of the selected classification guide. It also includes a Page menu, where you can edit or delete the current classification guide, or add topics to it. See Creating or Editing a Classification Topic (page 6-41).

3. Click **OK** to return to the Configure Classification Guide page.

Creating or Editing a Classification Topic

Permissions: The Admin.ClassificationGuide right is required to perform this action. This right is assigned by default to the 'rmaprivileged' and 'rmaadmin' roles.

1. Select **Configure—Classification—Configure Classification Guide** from the Configure Records Management Page (page 7-2).

   The Configure Classification Guide Page (page 6-44) is displayed.

2. In the dropdown list, select the classification guide to create the topic for, and click **Info**.

   The Classification Guide Information Page (page 6-46) is displayed.

3. From the Page menu, choose **Edit—Configure Topics**.

   The Administer Classification Topic Page (page 6-47) is displayed.

4. Click **Add**.

5. The Create or Edit Classification Topic Page (page 6-48) is displayed.

6. Provide a name and description for the classification topic, and click **Create** when you finish.

7. The Configure Topic Settings Page (page 6-50) is displayed.

   Provide default values for each of the metadata fields, and click **Submit Update** when you finish.

Use this procedure to edit an existing classification topic:

1. Select **Configure—Classification—Configure Classification Guide** from the Configure Records Management Page (page 7-2).

   The Configure Classification Guide Page (page 6-44) is displayed.

2. In the dropdown list, select the classification guide to edit and click **Info**.

   The Classification Guide Information Page (page 6-46) is displayed.

3. From the **Actions** dropdown menu, choose **Configure Topics**.

The Administer Classification Topic Page (page 6-47) is displayed.

4. From the **Topic Name** dropdown list, select the classification topic to edit, and click **Info**.

   The Classification Topic Information Page (page 6-51) is displayed.

5. From the **Actions** dropdown menu, choose **Edit**.

6. Edit the description for the classification topic, and click **Submit Update** when you finish.

   A “Successfully updated classification topic” screen is displayed.

7. Click **OK** to return to the Administer Classification Topic Page (page 6-47).

Editing Classification Topic Settings

Permissions: The Admin.ClassificationGuide right is required to perform this action. This right is assigned by default to the ‘rmaprivileged’ and ‘rmaadmin’ roles.

1. Select **Configure—Classification—Configure Classification Guide** from the Configure Records Management Page (page 7-2).

   The Configure Classification Guide Page (page 6-44) is displayed.

2. In the dropdown list, select the classification guide to edit topic settings for, and click **Info**.

   The Classification Guide Information Page (page 6-46) is displayed.

3. From the **Actions** dropdown menu, choose **Configure Topics**.

   The Administer Classification Topic Page (page 6-47) is displayed.

4. From the **Topic Name** dropdown list, select the classification topic whose settings to edit, and click **Info**.

   The Classification Topic Information Page (page 6-51) is displayed.

5. From the Page menu, choose **Edit—Edit Topic Settings**.

6. Modify the default metadata field values as required, and click **Submit Update** when you finish.

   The Edited Topic Settings screen is displayed.

7. Click **OK** to return to the Administer Classification Topic Page (page 6-47).

Deleting a Classification Topic

Permissions: The Admin.ClassificationGuide right is required to perform this action. This right is assigned by default to the ‘rmaprivileged’ and ‘rmaadmin’ roles.

1. Select **Configure—Classification—Configure Classification Guide** from the Configure Records Management Page (page 7-2).

   The Configure Classification Guide Page (page 6-44) is displayed.

2. In the dropdown list, select the classification guide whose topic to delete, and click **Info**.

   The Classification Guide Information Page (page 6-46) is displayed.

3. From the Page menu, choose **Configure Topics**.

   The Administer Classification Topic Page (page 6-47) is displayed.

4. From the **Topic Name** dropdown list, select the classification topic to delete, and click **Delete**.

   A message is displayed stating that the classification topic was deleted successfully.

5. Click **OK** to return to the Administer Classification Topic Page (page 6-47).

Viewing Classification Topic Information

Permissions: The Admin.ClassificationGuide right is required to perform this action. This right is assigned by default to the ‘rmaprivileged’ and ‘rmaadmin’ roles.

1. Select **Configure—Classification—Configure Classification Guide** from the Configure Records Management Page (page 7-2).

   The Configure Classification Guide Page (page 6-44) is displayed.

2. In the dropdown list, select the classification guide whose topic information is to be viewed, and click **Info**.

   The Classification Guide Information Page (page 6-46) is displayed.

3. From the Page menu, choose **Edit—Configure Topics**.

   The Administer Classification Topic Page (page 6-47) is displayed.

4. From the **Topic Name** dropdown list, select the classification topic to view, and click **Info**.

The Classification Topic Information Page (page 6-51) is displayed.

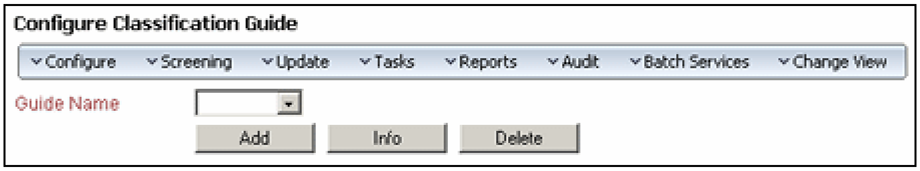
5. Click **OK** to return to the Administer Classification Topic Page (page 6-47).

Classification Guide Interface

The following screens are used to configure classification guides:

- Configure Classification Guide Page (page 6-44)
- Create or Edit Classification Guide Page (page 6-45)
- Classification Guide Information Page (page 6-46)
- Administer Classification Topic Page (page 6-47)
- Create or Edit Classification Topic Page (page 6-48)
- Configure Topic Settings Page (page 6-50)
- Classification Topic Information Page (page 6-51)

Configure Classification Guide Page



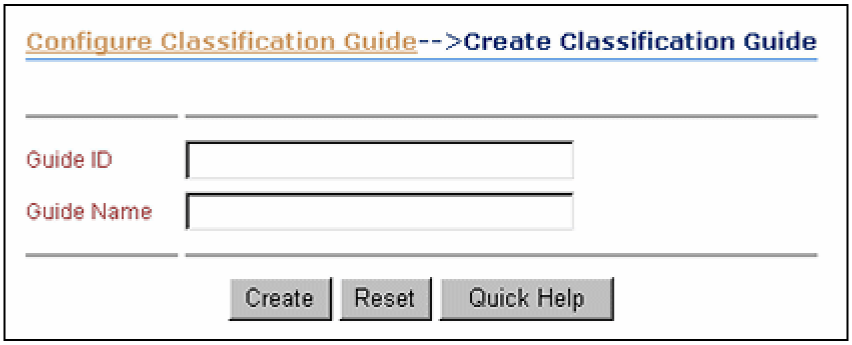
Permissions: The Admin.ClassificationGuide right is required to use this page. This right is assigned by default to the ‘rmaprivileged’ and ‘rmaadmin’ roles.

To access this page, select **Configure—Classification—Configure Classification Guide** from the Configure Records Management Page (page 7-2) page.

Feature	Description
Guide Name field	The dropdown list contains all defined classification guides. Use the **Info** button to view information about the selected classification guide or edit it, and the **Delete** button to delete it.
Add button	Displays the Create or Edit Classification Guide Page (page 6-45), used to create a new classification guide.

Feature	Description
Info button	Displays the information page for the selected classification guide. See Classification Guide Information Page (page 6-46).
Delete button	Click this button to delete the selected classification guide. See Deleting a Classification Guide (page 6-40).

Create or Edit Classification Guide Page


Configure Classification Guide-->Create Classification Guide
Guide ID
Guide Name
Create
Reset
Quick Help

Permissions: The Admin.ClassificationGuide right is required to use this page. This right is assigned by default to the ‘rmaprivileged’ and ‘rmaadmin’ roles.

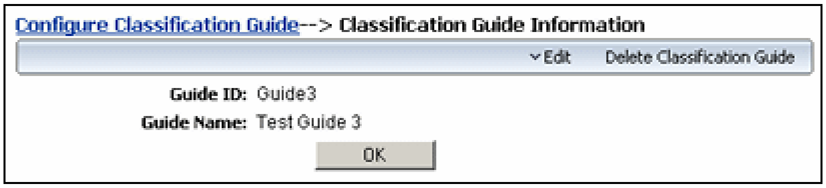
Use the Create page to define a new classification guide. To access this page, select **Configure—Classification—Configure Classification Guide** from the Configure Records Management Page (page 7-2).Click **Add**.

Use the Edit page to modify the name of an existing classification guide. To access this page, select **Configure—Classification—Configure Classification Guide** from the Configure Records Management Page (page 7-2). In the dropdown list, select the classification guide to edit, and click **Info**. From the **Actions** dropdown menu, choose **Edit**.

Feature	Description
Guide ID field	Enter an identifier for the classification guide. ❖ Required. ❖ Maximum characters: 80. This field is view-only on the edit page.

Feature	Description
Guide Name field	Enter a name or description for the classification guide. ❖ Required. ❖ Maximum characters: 100.
Create button (Create page only)	Creates the new classification guide.
Submit Update button (Edit page only)	Submits the edited classification guide.
Reset button	If you are creating a new classification guide, this resets the page to its initial default settings. If you are editing an existing classification guide, this returns your original settings.

Classification Guide Information Page


Configure Classification Guide--> Classification Guide Information

Guide ID: Guide3

Guide Name: Test Guide 3

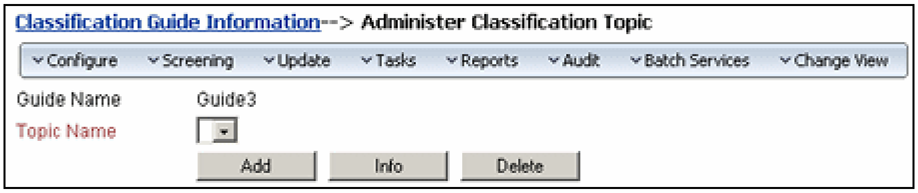
Permissions: The Admin.ClassificationGuide right is required to use this page. This right is assigned by default to the ‘rmaprivileged’ and ‘rmaadmin’ roles.

Configure—Classification—Configure Classification Guide from the Configure Records Management Page (page 7-2). In the dropdown list, select the classification guide to view and click **Info**.

Feature	Description
Guide ID field	Displays the identifier of the selected classification guide. This field cannot be edited.
Guide Name field	Displays the name of the selected classification guide. This field cannot be edited.

Feature	Description
Page menu	This menu has two main options: ❖ **Edit**—Used to edit the name of the current classification guide. See Creating or Editing a Classification Guide (page 6-39) for details. Also used to configure the topics associated with the current classification guide. See Administer Classification Topic Page (page 6-47). ❖ **Delete**—Used to delete the current classification guide. See Deleting a Classification Guide (page 6-40) for details.
OK button	Closes the page and returns you to the Configure Classification Guide Page (page 6-44).

Administer Classification Topic Page


Classification Guide Information--> Administer Classification Topic
Configure
Screening
Update
Tasks
Reports
Audit
Batch Services
Change View

Guide Name Guide3

Topic Name

Use this page to set up and configure classification topics.

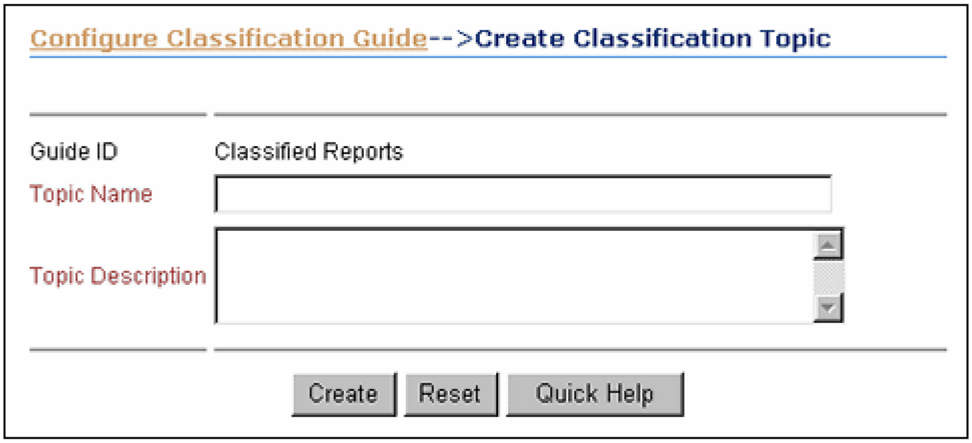
Permissions: The Admin.ClassificationGuide right is required to use this page. This right is assigned by default to the ‘rmaprivileged’ and ‘rmaadmin’ roles.

To access this page, select **Configure—Classification—Configure Classification Guide** from the Configure Records Management Page (page 7-2). In the dropdown list, select the classification guide to configure the topics for, and click **Info**. From the Page menu, choose **Edit—Configure Topics**.

Feature	Description
Guide Name field	This field shows the name of the classification guide that the topic is associated with. It cannot be edited.
Topic Name field	The dropdown list contains all defined topics for the current classification guide.

Feature	Description
Add button	Displays the Create or Edit Classification Topic Page (page 6-48), used to create a new classification topic.
Info button	Displays the Classification Topic Information Page (page 6-51).
Delete button	Click this button to delete the selected classification topic. See Deleting a Classification Topic (page 6-43).

Create or Edit Classification Topic Page



Configure Classification Guide-->Create Classification Topic

Guide ID Classified Reports

Topic Name

Topic Description

Permissions: The Admin.ClassificationGuide right is required to use this page. This right is assigned by default to the ‘rmaprivileged’ and ‘rmaadmin’ roles.

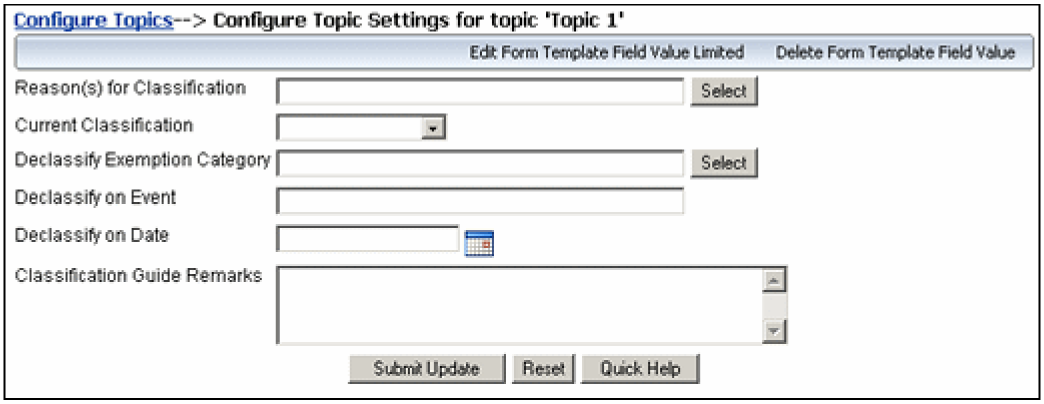
Use the Create page to define a new classification topic. To access this page, select **Configure—Classification—Configure Classification Guide** from the Configure Records Management Page (page 7-2). In the dropdown list, select the classification guide to create the topic for, and click **Info**. From the Page menu, choose **Edit—Configure Topics**. Click **Add** on the Administer Classification Topic Page (page 6-47).

Use the Edit page to modify the properties of an existing classification topic. To access this page, select **Configure—Classification—Configure Classification Guide** from the Configure Records Management Page (page 7-2). In the dropdown list, select the classification guide topic to edit and click **Info**. From the Page menu, choose **Edit—Configure Topics**. From the **Topic Name** dropdown list, select the classification topic to edit, and click **Info**. From the Page menu, choose **Edit**.

To modify the topic settings (i.e., the default metadata field values), you must choose **Edit Topic Settings** from the Page dropdown menu. This displays the Configure Topic Settings Page (page 6-50).

Feature	**Description**
Guide ID field	The name of the classification guide that the topic is associated with. It cannot be edited.
Topic Name field	Enter a name for the classification topic. ❖ Required. ❖ Maximum characters: 255. This field is not displayed on the Edit screen.
Topic Description field	Enter a description for the classification topic. ❖ Required. ❖ Maximum characters: 1,000.
Create button (Create page only)	Creates the new classification topic and takes you to the Configure Topic Settings Page (page 6-50), where you can specify the default metadata field values.
Submit Update button (Edit page only)	Submits the edited classification topic properties and takes you back to the Administer Classification Topic Page (page 6-47).
Reset button	If you are creating a new classification topic, this resets the page to its initial default settings. If you are editing an existing classification topic, this returns your original settings.

Configure Topic Settings Page


Configure Topics--> Configure Topic Settings for topic 'Topic 1'
Edit Form Template Field Value Limited
Delete Form Template Field Value
Reason(s) for Classification
Select
Current Classification
Declassify Exemption Category
Select
Declassify on Event
Declassify on Date
Classification Guide Remarks
Submit Update
Reset
Quick Help

Permissions: The Admin.ClassificationGuide right is required to use this page. This right is assigned by default to the ‘rmaprivileged’ and ‘rmaadmin’ roles.

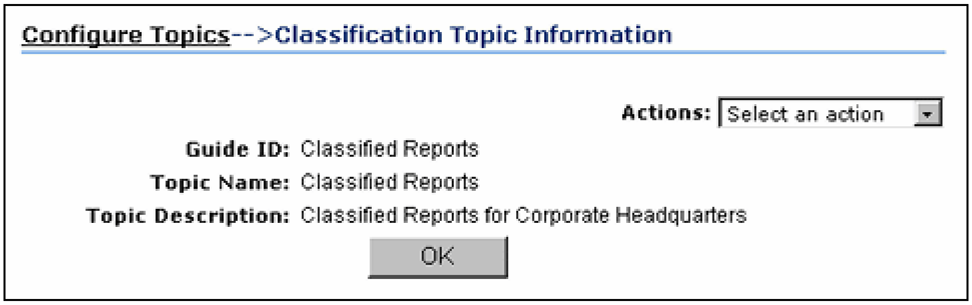
Use this page to set or modify the default field values of a classification topic. To access this page, select **Configure—Classification—Configure Classification Guide** from the Configure Records Management Page (page 7-2). In the dropdown list, select the classification guide to edit topic settings for, and click **Info**. From the Page menu, choose **Edit—Configure Topics**. From the **Topic Name** dropdown list, select the classification topic settings to edit, and click **Info**. From the Page menu, choose **Edit—Edit Topic Settings**.

To modify the topic name and/or description, choose **Edit** from the **Actions** dropdown menu. This displays the Create or Edit Classification Topic Page (page 6-48).

Feature	Description
Initial classification	Select the initial classification of records assigned to the topic. The dropdown list contains all defined classification levels. **Note:** You will only see the classification levels that you are entitled to see. For example, if your assigned classification level is ‘Secret’, the dropdown list only shows ‘Secret’ and all lower classification levels. Similarly, if no classification level was assigned to you, you will see ‘No Markings’.

Feature	Description
Reason(s) for classification	Specify the default reason(s) for classification of records assigned to the topic. The dropdown list contains the classification reasons defined by the content server system administrator using the Configuration Manager utility.
Declassify exemption category	Select the default declassification exemption category of records assigned to the topic. The dropdown list contains the declassification exemption categories defined by the content server system administrator using the Configuration Manager utility.
Declassify on event	Select the default declassification event of records assigned to the topic. The dropdown list contains the declassification events defined by the content server system administrator (using the Configuration Manager utility).
Declassify on date	Click the calendar icon next to the field to select the default scheduled declassification date of records assigned to the topic.
Classification Guide Remarks	If required, specify additional remarks about the classification guide to clarify its usage, etc.
Submit Update button	Sets the default metadata field values as specified.
Reset button	If you are creating a new topic, this resets the page to its initial default settings. If you are editing an existing topic, this returns your original settings.

Classification Topic Information Page



Configure Topics-->Classification Topic Information

Guide ID: Classified Reports

Topic Name: Classified Reports

Topic Description: Classified Reports for Corporate Headquarters

Permissions: The Admin.ClassificationGuide right is required to use this page. This right is assigned by default to the ‘rmaprivileged’ and ‘rmaadmin’ roles.

To access this page, select **Configure—Classification—Configure Classification Guide** from the Configure Records Management Page (page 7-2). In the dropdown list, select the classification guide topic information to see, and click **Info**. From the **Actions** dropdown menu, choose **Configure Topics**. From the **Topic Name** dropdown list, select the classification topic information to view, and click **Info**.

Feature	Description
Guide ID field	This field shows the name of the classification guide that the topic is associated with. It cannot be edited.
Topic Name field	This field shows the name of the classification topic. It cannot be edited.
Topic Description field	This field shows the description of the classification topic. It cannot be edited.
Actions dropdown menu	This dropdown menu has these options: ❖ **Edit**—Used to edit the name and/or description of the current classification topic. ❖ **Delete**—Used to delete the current classification topic. See Deleting a Classification Topic (page 6-43). ❖ **Edit Topic Settings**—Used to edit the topics settings. See Editing Classification Topic Settings (page 6-42).
OK button	Closes the page and returns you to the Administer Classification Topic Page (page 6-47).

Chapter

7

GENERAL CONFIGURATION OPTIONS

OVERVIEW

This chapter is for records administrators who are responsible for configuring DoD Edition (generally those with the ‘rmaadmin’ role). Certain configuration procedures described here and in other chapters may also apply to other users if they have been given the appropriate rights. The required rights are noted for each procedure.

This chapter covers the following topics:

- ❖ Configuring Records Management (page 7-1)
- ❖ Configuring the Root Nodes (page 7-12)
- ❖ Configuring the Root Nodes (page 7-12)
- ❖ Configuration Variables (page 7-13)

CONFIGURING RECORDS MANAGEMENT

A number of system-wide configuration settings for the DoD Edition environment are specified on theConfigure Records Management Page (page 7-2). This chapter discusses the following configuration screens and tasks.

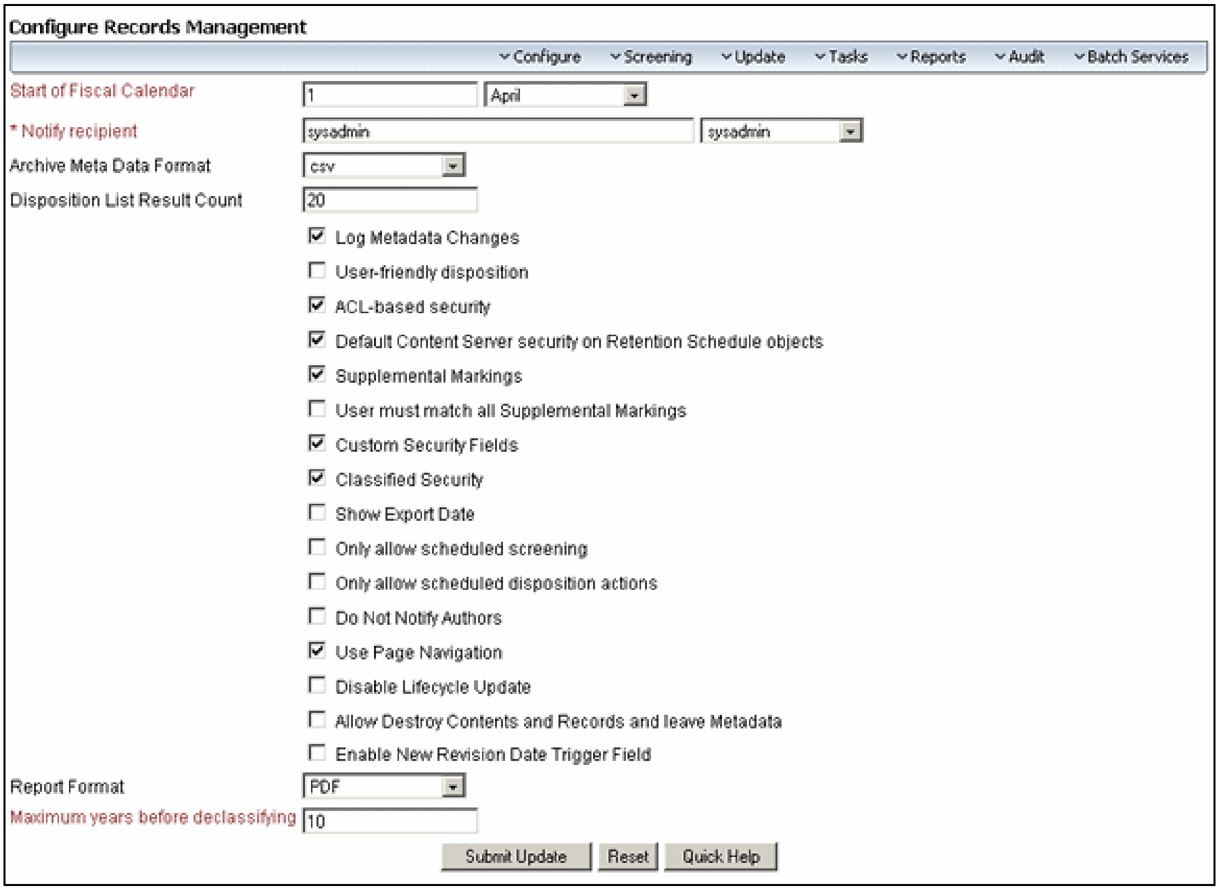
- ❖ Configure Records Management Page (page 7-2)
- ❖ Setting the Fiscal Calendar (page 7-10)
- ❖ Setting the Default Notification Recipient(s) (page 7-11)

Configure Records Management Page

Use this page to set most of the configuration options for your system. To access this page, select **Configure Records Management** from the **Administration** tray.

Permissions: The Admin.RecordManager right is required to use this page. This right is assigned by default to the ‘rmaadmin’ role.

Figure 7-13 Configure Records Management page



Start of Fiscal Calendar	1 April
* Notify recipient	sysadmin sysadmin
Archive Meta Data Format	csv
Disposition List Result Count	20

☑ Log Metadata Changes

□ User-friendly disposition

☑ ACL-based security

☑ Default Content Server security on Retention Schedule objects

☑ Supplemental Markings

□ User must match all Supplemental Markings

☑ Custom Security Fields

☑ Classified Security

□ Show Export Date

□ Only allow scheduled screening

□ Only allow scheduled disposition actions

□ Do Not Notify Authors

☑ Use Page Navigation

□ Disable Lifecycle Update

□ Allow Destroy Contents and Records and leave Metadata

□ Enable New Revision Date Trigger Field

Report Format	PDF
Maximum years before declassifying	10

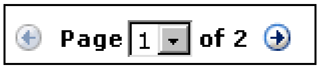
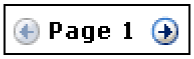
Feature	Description
Start of Fiscal Calendar	Specify the date by typing the day of the month and selecting the month from the dropdown list. ❖ Required for processing fiscal date periods. ❖ Initial default: April 1.
Notify recipient	Specify the user name(s) of the person(s) responsible for reviewing records folders, records and non-record content, and pending disposition events. E-mail notifications are sent to the person when it is time to review a record/non-record content item or process a pending event. To specify more than one person, separate them with commas. All persons selected for default notification should be assigned the 'rmaadmin' role. See Setting the Default Notification Recipient(s) (page 7-11).
Archive Meta Data Format	Specify the file format that the metadata for items in a disposition bundle (for example, a zipped archive of items affected by a transfer, archive, or accession disposition action created using the Get Content, Records and Folders command) will be stored in. There are three options: • hda—This archives the metadata in Oracle's proprietary HDA file format, which is specific to Content Server. • xml—This archives the metadata in the eXtensible Markup Language (XML) format, which can be read and processed further by other applications. • csv—(initial default) This archives the metadata in the comma-separated values (CSV) format, which can be read by Microsoft Excel and other applications.

Feature	Description
Disposition List Result Count	Specify the maximum number of items that are displayed. ❖ Initial default: 20. ❖ If the list contains more items than displayed, navigation controls are added to move between pages.
Log Metadata Changes	Select this check box to enable tracking item-level metadata changes. Any changes to the item metadata are accessible via the Metadata History command in the Actions dropdown menu on the content information page of the record. ❖ Initial default: enabled.
User-friendly disposition	Select this check box to enable more user-friendly language for disposition rules. Clear this check box for standard DoD 5015 disposition and screening query language. The disposition captions are displayed in the Disposition Information page and Disposition Rule screen. ❖ Initial default: not enabled (i.e., standard disposition and query language is used).
ACL-based security	This setting enables security based on access control lists (ACLs). It enables the Group and User Permissions fields on the Create/Edit Retention Category, Records Folder, and Trigger pages, where you can create access control lists to assign security permissions. ❖ Initial default: enabled.

Feature	Description
Default Content Server security on Retention Schedule objects	This setting enables the default Content Server security on retention categories, records folders, and triggers. It enables the standard Security Group and Filer fields on the Create and Edit Retention Category, Records Folder, Custom Disposition Action, Freeze, and Triggers screens, so that you can assign additional security on those retention schedule objects and components. ❖ Initial default: enabled. **Tech Tip:** Do not change this setting after your production environment is under way. If your organization requires a change to this feature after your production environment is running, call Technical Support for assistance.
Supplemental Markings	Available for records only. This setting enables supplemental marking security on records, records folders, and records users. This check box must be selected to enforce user matching of at least one supplemental marking. ❖ Initial default: enabled (i.e., supplemental markings security is enabled). **Note:** The **Supplemental Markings** check box must be enabled for the “User must match all Supplemental Markings” feature to function. For more information, see Supplemental Markings (page 6-3).

Feature	Description
User must match all Supplemental Markings	Available for records only. When enabled, this option forces a user to match all supplemental markings in force to access a record. When not selected, a user must match at least one supplemental marking to access a record within a marked records folder. ❖ Initial default: not enabled (i.e., user must match one or more supplemental markings to access a records folder or records). **Note:** The **Supplemental Markings** check box must be enabled for this feature to work.
Custom Security Fields	Available for records only. Select this check box to enable the custom security field feature. When you enable this field, the Custom Security Field is displayed in the Configure menu. For more information, see Custom Security Fields (page 6-27). Clear this check box if you do not have a need for this feature. ❖ Initial default: not enabled.

Feature	Description
Classified Security	Available for records only. Select this check box to enable the classified security feature as required for agencies conforming to the Chapter 4 Classified Records section of DoD 5015.2 specification. For more information, see Security Classifications (page 6-13). When enabled, the Security Classification Field is displayed in the Configure menu. After you create the classification levels and assign them to yourself, you must set order on the hierarchy levels. See Setting the Order of Security Classifications (page 6-19). Clear this check box if your agency or organization does not require this feature. ❖ Initial default: enabled/disabled, depending on whether the Classified Enhancements option was selected during DoD Edition installation.
Show Export Date	Select this check box to enable users to export items in the retention schedule that have changed since a specific date. ❖ Initial default: not enabled (i.e., date field not displayed).
Only allow scheduled screening	Select this check box to allow only scheduled screening reports rather than to permit users to start them manually. This option hides the “Search” button on the screening page so all screening requests must be scheduled. This is useful in environments where the total number of records in the system is so large that it is impractical to have users wait for screening reports. ❖ Initial default: not enabled (i.e., manual screening is allowed).

Feature	Description
Only allow scheduled disposition actions	Select this check box to allow only scheduled disposition actions rather than permit users to start them manually. Users are only able to perform their pending records assignments by scheduling them. This is useful in environments where disposition actions typically take too long to have users waiting for them. ❖ Initial default: not enabled (i.e., manual disposition actions are allowed).
Do Not Notify Authors	Select this check box if you do not want e-mail notifications to be sent for pending events, reviews, and the Notify Authors disposition action. ❖ Initial default: not enabled (i.e., e-mail notifications are sent).
Use Page Navigation	Select this check box to display more elaborate page navigation controls (including the total number of pages) on the screening results lists and the disposition record folder lists. ❖ Initial default: enabled (i.e., more elaborate page navigation is used). Page navigation on:  Page 1 of 2 Page navigation off:  Page 1

Feature	Description
Maximum years before declassifying	Enter the number of years after which records will be declassified. ❖ Initial default: 10 years. **Permissions:** This field is only displayed if the classified security features have been enabled in DoD Edition and you have the Admin.PrivilegedEnvironment rights. This right is assigned by default to the predefined 'rmaprivileged' and 'rmaadmin' role.
Disable Lifecycle Update	This option stops the updating of disposition dates and review date computation and the update for changed or new content items. This setting can be used when uploading large batches of data.
Allow Destroy Contents and Records and leave Metadata	If checked, when contents are destroyed the metadata field is still retained. If not checked, the metadata field is destroyed with the content.
Enable New Revision Date Trigger Field	If checked, this creates a custom metadata field of New Revision Date. When a new revision of a content item is checked in, the field is updated with the new revision's checked-in date.
Submit Update button	Submits your updated configuration settings.
Reset button	Resets the page to its initial default settings.
Quick Help button	Displays help information about this page.

Configuration Page Menus

The remaining chapters in this guide discuss how to configure the other components that interact with the record objects in your retention schedule. The retention schedule components that you must configure for your retention schedule include defining triggers for triggering time, event, and time-event dispositions, customizing periods for review cycles and retention periods, and creating supplemental markings to assign to users, folders, and records for increased security. The triggers and periods are used for disposition processing rules. Supplemental markings and custom security fields further restrict access to records objects, such as records folders and retention categories.

The Configure menu at the top of the Configure Records Management Page (page 7-2) is used to configure the majority of functionality for DoD Edition. Depending on the products chosen at installation, different options can appear. The following list describes all options that are possible:

- Disposition Actions: used to access a menus to create custom dispositions and to disable dispositions.
- Classification: used to set up Classification Guides and security classifications. See Security Classifications (page 6-13) for details.
- Triggers: used to set up triggers, which are associated with the disposition rules for items. See Chapter 9 *(Setting up Triggers)* for complete instructions.
- Periods: used to set up the time periods used in dispositions. See Chapter 10 *(Configuring Time Periods)* for complete instructions.
- Supplemental Markings: used to add supplemental markings which can further clarify document handling. See Supplemental Markings (page 6-3) for complete details.
- Custom Security Fields: used to create custom fields to be used to further enhance security. See Custom Security Fields (page 6-27) for details.
- Freezes: used to configure freezes for dispositions. See Chapter 12 *(Configuring Dispositions and Freezes)* for details.
- Root Nodes: used to set up the root node, which is the basis of the retention schedules. See Configuring the Root Nodes (page 7-12) for details.
- Metadata Sets: used to access menus to configure custom metadata for your system. See Chapter 11 *(Custom Metadata Fields)* for details.
- Profiles: used to access menus to configure profiles for use on the system.
- Related Content Types: used to set up links between content. See Chapter 13 *(Configuring Related Content (Links))* for details.

The other menus (Reports, Audit, Screening, and so on) are all discussed in the Records Manager DoD Edition System Maintenance Guide.

Setting the Fiscal Calendar

The fiscal calendar is the calendar used by your organization for financial and accounting purposes. A fiscal year may coincide with a calendar year (i.e., run from January 1 to

December 31), but it does not need to. You can set your own fiscal calendar (for example, running from April 1 to March 31).

You need to specify the start date of your fiscal year only once, unless your organization changes their fiscal start date or the start date varies from year to year. You might also have to set the fiscal start date 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.

Permissions: The Admin.RecordManager right is required to perform this task. This right is assigned by default to the ‘rmaadmin’ role.

To set your fiscal calendar start date, complete the following steps:

1. Select **Configure Records Management** from the **Administration** tray.

   The Configure Records Management Page (page 7-2) is displayed.

2. Specify the date the fiscal year begins for your organization in the **Start of Fiscal Calendar** box. To enter a date, enter the starting date and select the month from the dropdown 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 is displayed saying that configuration was successful.

4. Click **OK**.

Setting the Default Notification Recipient(s)

Permissions: The Admin.RecordManager right is required to perform this action. This right is assigned by default to the ‘rmaadmin’ role.

E-mail notifications are sent to users indicating that records or non-record content items require reviewing and marking as reviewed, or that a pending disposition event requires attention. Persons designated as the default recipients are able to view the pending records or non-record content items for review, records folders for review, and disposition events of other users. The pending actions of other users are contained in the Other Assignments link in the My Content Server—My Retention Assignments area. For further information about processing retention assignments, see the *Records Manager DoD Edition System Maintenance Guide*.

Permissions: You can also set the users who receive review and disposition schedule notifications at the retention category and records folder level. Any reviewers indicated specifically for a record or non-record content item, records folder, or retention category also receive notification in addition to the system default recipient(s). The users you select as the default notification recipients must have the Admin.PerformActions and Admin.PerformPendingReviews rights.

Note: You can also specify a notification reviewer for each disposition rule. For further details, see Disposition Rule Screen (page 14-25).

To set one or more default notification recipients, complete the following steps:

1. Select **Configure Records Management** from the **Administration** tray.

   The Configure Records Management Page (page 7-2) is displayed.
2. In the **Notify recipient** box, specify one or more users who will be the default recipients for notifications. You can enter their user names separated by commas, or select one or more users from the dropdown list on the right.
3. Click **Submit Update**.

   A message is displayed saying that configuration was successful.
4. Click **OK**.

Configuring the Root Nodes

In the Configure Root Nodes page, you can view information about the top series node of the retention schedule. You can also hide the series, or generate a retention schedule report. This is especially useful when you are setting up a new retention schedule or areas of a retention schedule.

Tech Tip: You can generate a retention schedule report for the entire retention schedule from the Configure Root Nodes page, because it contains the top-level node.

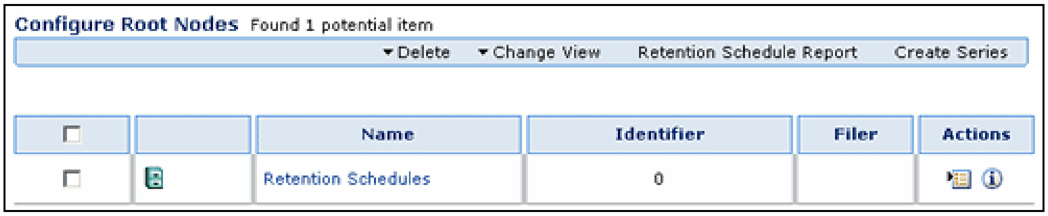
Permissions: The Admin.RecordManager right is required to configure the root nodes. This right is assigned by default to the ‘rmaadmin’ role.

You can configure the root series nodes for your retention schedule on the Configure Root Nodes page. This page displays the top level parent node of the retention schedule. To access this page, complete the following steps:

1. Select **Configure—Root Nodes** from the Configure Records Management Page (page 7-2).

   Figure 7-14 is displayed.

Figure 7-14 Configure Root Nodes page



Configure Root Nodes Found 1 potential item

☐		Name	Identifier	Filer	Actions
☐		Retention Schedules	0		☰ ⓘ

The Page menu and the Actions icon (☰) popup menu for each root node have the following options:

- **Delete:** Deletes either the series or the tree. If a multiple nodes are selected, the Delete option on the Page menu will delete all selected nodes. The topmost root series does not have a parent series, because it is the root node. The information field **Is Root** is always “Yes” for this series, and the Parent Identifier is always “0”.
- **Change View** (Page menu only): Changes the layout from Headline view (as shown) to Thumbnail view.
- **Retention Schedule Report**: Generates a retention schedule report for the *entire* retention schedule under the root node. For more information about retention schedule reports, see the *Records Manager DoD Edition User Guide*.
- **Create Series**: Enables you to create a series at that node level. For more information, see Creating or Editing a Series (page 8-16).

CONFIGURATION VARIABLES

A number of configuration variables are available that can be included (or modified) in DoD Edition’s configuration file to change the behavior or interface of the application. The configuration file is located at <*CS_Instance_Dir*>/ custom/RecordsManagement/records_management_environments.cfg.

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 checkin and update for email records. The flags are a double-colon-separated list.

The following section describes some of the more commonly used configuration variables.

UieHideSearchCheckboxes

Use this configuration variable 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.

- `UieHideSearchCheckboxes=true:` The metadata field check boxes are not shown on the search page.
- `UieHideSearchCheckboxes=false:` The metadata field check boxes are shown on the search page.

The default setting is `TRUE`, so the metadata field check boxes are not displayed.

You must restart the content server for this setting to take effect.

RmaNotifyDispReviewerAndCatAuthor

By default, when events are triggered by a disposition rule, both the specified notification reviewer and the original category author receive e-mail notifications about the event. You can use this configuration variable to control who is notified.

- `RmaNotifyDispReviewerAndCatAuthor=true:` Both the specified notification reviewer and the category author receive e-mail notifications.

- `RmaNotifyDispReviewerAndCatAuthor=false:` Only the category author receives e-mail notifications.

The default setting is `TRUE`, so both the specified notification reviewer and the category author receive e-mail notifications.

You must restart the content server for this setting to take effect.

RmaNotifyReviewerAndAlternateReviewer

Users can select an alternate user to perform review actions and process assigned disposition events, for example if they are out of the office for some time. By default, both the original user and the alternative reviewer receive e-mail notifications about the action.You can use this configuration variable to control who is notified.

- `RmaNotifyReviewerAndAlternateReviewer=true:` Both the specified alternative reviewer and the original user receive e-mail notifications.
- `RmaNotifyReviewerAndAlternateReviewer=false:` Only the alternative reviewer receives e-mail notifications.

The default setting is `FALSE`.

You must restart the content server for this setting to take effect.

RecordsManagementNumberOverwriteOnDelete

Use this configuration variable to set the number of disk scrubbing passes used for a destroy action.

- `RecordsManagementNumberOverwriteOnDelete=`*Number:* Where *Number* is the number of passes.

The default number of scrubbing passes is 2.

You must restart the content server for this setting to take effect.

RMAHideExternalFieldsFromSearchInfo

Use this configuration variable to hide external fields on the Search and Info pages. The default setting is TRUE, meaning that External fields are hidden on those screens.

- `RMAHideExternalFieldsFromSearchInfo=true:` This hides the external fields on the Search and Info pages.

- `RMAHideExternalFieldsFromSearchInfo=false:` This displays the external fields on the Search and Info pages.

You must restart the content server for this setting to take effect.

RMAHideExternalFieldsFromCheckInUpdate

Use this configuration variable to hide external fields on the Checkin and Update pages. The default setting is TRUE, meaning that External fields are hidden on those screens.

- `RMAHideExternalFieldsFromCheckInUpdate=true:` This hides the external fields on the Checkin and Update pages.
- `RMAHideExternalFieldsFromSearchInfo=false:` This displays the external fields on the Checkin and Update pages.

You must restart the content server for this variable to take effect.

AllowRetentionPeriodWithoutCutoff

This variable allows you to specify retention periods for triggers for record and non-record content items. To use this functionality, you must add this variable to the records_management_environments.cfg file.

- `AllowRetentionPeriodWithoutCutoff=true`: retention periods for triggers for non-record content items are enabled.
- `AllowRetentionPeriodWithoutCutoff=false`: retention periods are disabled.

You must restart the content server for this variable to take effect.

RmaAddDocWhereClauseForScreening

This variable allows users with the rmaadmin role to screen for frozen items to which they do not have access (via ACLs) on the screening page or on the Freeze Information Page (page 12-27).

- `RmaAddDocWhereClauseForScreening=false`: frozen items can be screened. Default.
- `RmaAddDocWhereClauseForScreening=true`: frozen items cannot be screened.

The default is `FALSE`.

ShowCreateExternalMenu

This variable exposes menu selections to create and use external records.

- `ShowCreateExternalMenu=TRUE`: menu selections are exposed.
- `ShowCreateExternalMenu=FALSE`: menu selections are hidden.

RecordsManagementDenyAuthorFreePassOn RMSecurity

This variable allows the author of content to delete content they authored regardless of the user's security settings.

- `RecordsManagementDenyAuthorFreePassOnRMSecurity=TRUE`: Authors are not allowed to delete content they authored.
- `RecordsManagementDenyAuthorFreePassOnRMSecurity=FALSE`: Authors are allowed to delete content they authored.

The default is FALSE.

Chapter

8

Setting Up a Retention Schedule

Overview

Important: If you have installed a DoD compliant version of Records Manager DoD Edition, the term “File Plan” is used in place of “Retention Schedule” in your interface.

This section describes how to set up and administer the retention schedule for an organization. It covers the following topics:

Concepts

- About Retention Schedules (page 8-3)
- Using a Series (page 8-15)
- Retention Categories (page 8-21)
- Records Folders (page 8-30)

Tasks

- Creating or Editing a Series (page 8-16)
- Viewing Series Information (page 8-17)
- Hiding and Unhiding a Series (page 8-17)
- Moving a Series (page 8-18)

Examples

Interface

About Retention Schedules

Important: If your retention schedule contains 10,000 or more series, categories, and folders, then your database administrator should build database indices on the tables to enhance performance. For records folders, add indices on the columns of the Folders table. For retention categories, add indices on the columns of the Categories and Dispositions tables. For series, add indices on the columns of the Series table. For further information about defining an index on a table column, see your database documentation.

A retention schedule is an organized hierarchy of series, categories, and folders, which allows you to cluster records and non-record content items into similar groups, each with its own retention and disposition characteristics. In Records Manager DoD Edition, you can create as many retention schedules as necessary for the requirements mandated by your organization.

If a records folder does not have its own security settings, the records folder inherits security settings from its parent retention category. Each records folder can have its own security settings that further limit access to the records in that folder. Records folders can be further secured by using supplemental markings and custom security fields.

Records folders also inherit disposition rules from their retention category. By default, all records folders within a retention category inherit disposition instructions from the category. A disposition rule defined within a category can be applied to a specific records folder, if that folder has a unique disposition instruction.

Records folders for temporary records are destroyed with temporary records as part of final disposition processing. Records administrators create new records folders as necessary to accommodate processing temporary records. Records folders for records subject to review and permanent records are not destroyed, and do not have to be recreated due to final disposition.

Important: The retention schedule is not a contribution mechanism, but rather a disposition mechanism. It defines how and when records and non-record content items should be processed during their lifecycle. It is not intended to check records or content items into the content server.

Planning Your Retention Schedule

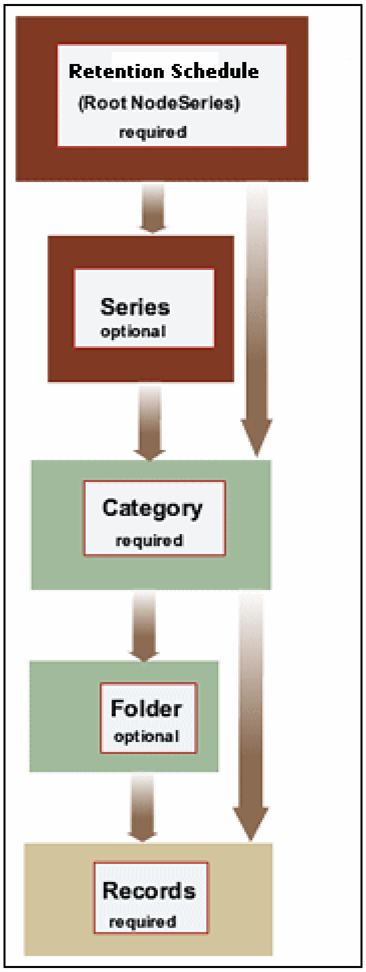
Do not base a category on a dynamic feature such as organization hierarchy because organizations are reorganized on a frequent basis. Use static divisions for category departments, and be more generic with categories. Records folders can be more specific.

You should plan to set up separate retention schedules for record items and non-record content items. Disposition instructions for non-record content items are usually different than those for record items. It is simpler to track items when they are sorted into appropriate categories.

Retention Schedule Hierarchy

A typical hierarchy of a retention schedule consists of series, categories, and/or 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. Records folders can be nested. The following figure shows the basic hierarchy of retention schedule objects.

Figure 8-1 Basic retention schedule hierarchy

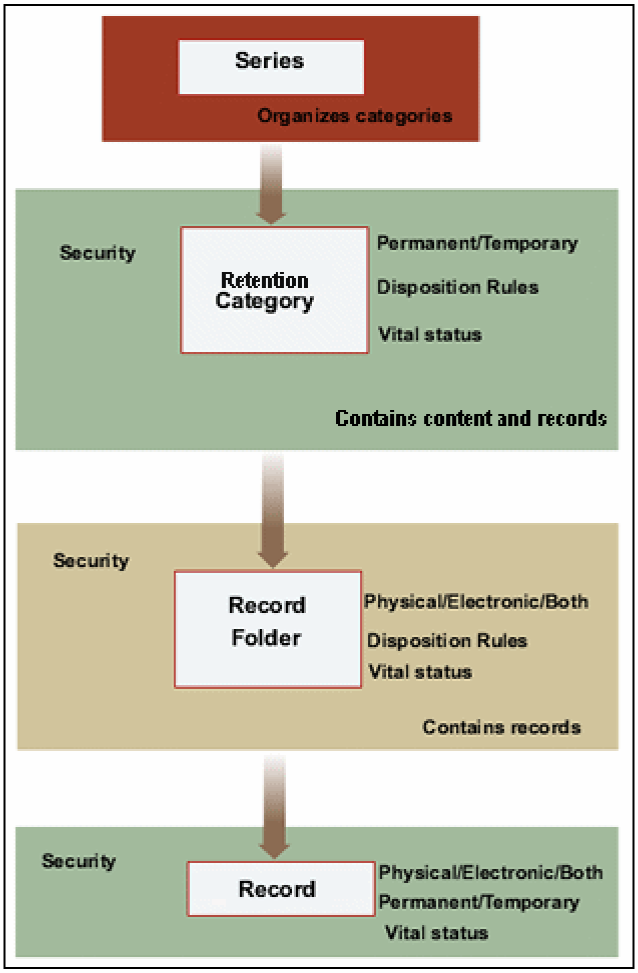


Records and non-record content items are filed directly into a retention category, and records can optionally be filed into a records folder under a retention category. The retention schedule is the top-most series root node. The top node is created automatically for you by the DoD Edition component.

The remaining retention schedule objects—series or records folder or retention category—are created by the records administrator. Records users or administrators create records and non-record content items 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 and records. A records folder is optional, and it also organizes records according to some commonality. For obvious reasons, content items are a required constituent of the retention schedule.

The figure below 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, records folders, and records all have a variety of security options, including access control lists (ACLs), supplemental markings, custom security fields, and (custom) classifications.

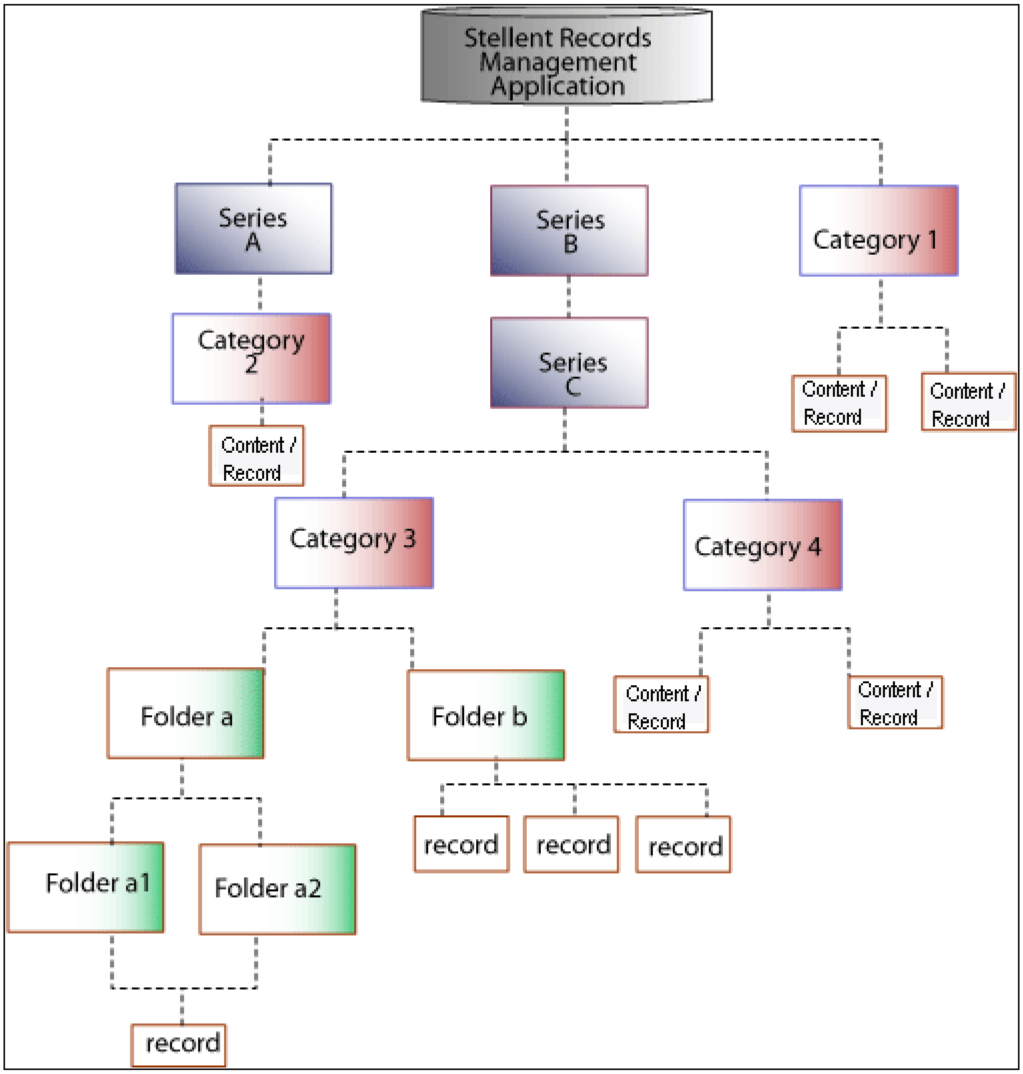
Figure 8-2 Attributes of retention schedule objects



The following figure 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 and records filed directly into a category (Categories 1, 2, and 4) rather than a folder
- categories without a series (Category 1)
- a record filed into multiple folders (Folders a1 and a2).

Figure 8-3 Sample retention schedule hierarchy



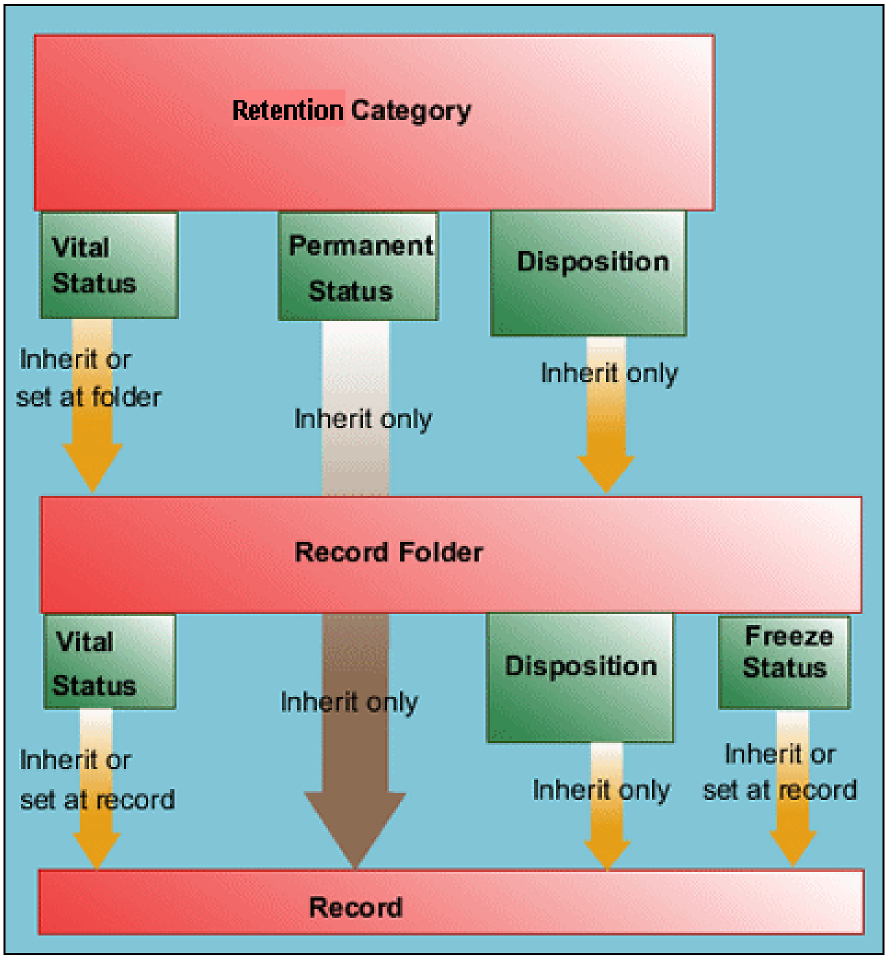
While it is possible to file records and non-record content items into multiple locations in the retention schedule, this is not recommended due to the complexity of processing multiple disposition schedules. For best performance results, records should be filed into a single folder or category. Likewise, non-record content should be filed into a singular category. When multiple disposition schedules are attached to an item, the item is processed by the disposition with the longest retention period.

Attribute Inheritance

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. This figure shows at what levels certain characteristics (attributes) of a content or records object are specified.

Some security settings are inherited and overridden as well, which is explained in Chapter 5 (*Setting Up Security)*.

Figure 8-4 Inherited attributes



Review Status Attributes

Review status, which includes the review period and reviewer, can be set at the retention category level, record folder level (for records, not for non-records), 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 and records information pages. DoD Edition essentially ignores the longer review period; however, if the shorter review period is removed or changed, the longer review period reigns again in cycling reviews for records and non-record content.

Important: 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 category that is subject to review has a review period of two calendar quarters. A child folder within the category that is subject to review has a review period set as four calendar quarters. Because the category higher up in the hierarchy, or 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 you do not set review status at the record folder level for a record folder that exists within a record category that is subject to review, the record folder *always* inherits review record status from the record category. At the content or record level, a content or record can inherit review record information from the category, and the record can inherit information from the folder if it does not have its own review settings. If a content item or record is filed directly into a retention category that is subject to review, it inherits settings from the category. If a record that is subject to review is filed into a records folder that is subject to review, it inherits record settings from the immediate parent record folder. Because records folders can be nested, the immediate record folder parent determines review record attributes for the record.

If a retention category is subject to review, and none of the record folders or content items/records have their own review settings, then the record folders and the items all inherit review record attributes from the record category.

You can create a non-review retention category that can contain record folders, content, and records subject to review; however, the reverse is not possible: you cannot create a retention category that is subject to review that contains non-subject to review record folders and items due to inheritance of the subject to review attributes.

Permanent Record Status Attributes

Note: Permanent status applies to records only and not to non-record content.

The previous figure shows that the permanent record status is set at the category level only, and record folders and records inherit the record folder status. Permanent records cannot be destroyed by a disposition instruction. Permanent records typically are a small percentage of an organization's record base. Permanent record 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 records are sometimes referred to as "archival" records.

Disposition Instructions

Disposition instructions are defined at the retention category level, with some rules being applied uniquely to a child records folder. A records folder inherits disposition rules from the retention category. Records and non-record content items inherit dispositions from their retention category, and if applicable, a record folder with its own uniquely applied disposition rule. For more information, see Chapter 14 (*Defining Disposition Instructions)*.

Frozen Folder, Record, and Non-Record Content Status

Freezing a records folder inhibits disposition processing for that records folder and its child records folders and records.

Records folders and records or non-record content items inherit the freeze status if it is present on an ancestor. In addition to inheriting the freeze status, you can freeze at lower levels within a hierarchy where inheritance is not present; that is, you can freeze a child records folder or a record within a records folder.

Freezing a record or non-record content item that is outside of a folder also inhibits disposition processing.

Creating and Navigating Object Levels

You must be at a certain context, or level, within the retention schedule to work with retention schedule objects. Depending on your location within the hierarchy, different menu options appear in the main Actions list when browsing the retention schedule. The table below shows what retention schedule objects you can create at each level.

At this level:	You can create:
Series or root node	❖ Series ❖ Retention category
Retention category	❖ Record folder ❖ Record or non-record content item
Record folder	❖ Record folder ❖ Record

Retention Schedule Menus

Menus are relative to the location in the hierarchy. For example, at the Folder level you can create a folder or a record. You cannot create a category.

The following list describes the possible menu options which may appear depending on the location in the hierarchy. Information in parenthesis indicates the area of the hierarchy where the information appears:

- **Information**
  - Category Information (Category level): displays the Retention Category Information Page (page 8-48).
  - Series Information (Series level): displays the Series Information Page (page 8-40).
  - Folder Information (Folder level): displays the Records Folder Information Page (page 8-58).
  - Metadata History (Category level and Folder level): displays the Metadata History Page (page 8-48).
  - Disposition Information (Category level): displays the Disposition Information Page (page 14-28).
  - Life Cycle (Folder level): displays Life Cycle information. See the *Records Manager DoD Edition System Maintenance Guide* for details.
  - Recent Reviews (Folder level): displays review history information. See the *Records Manager DoD Edition System Maintenance Guide* for details.
  - Retention Schedule Report (all): creates a retention schedule report in the format specified when the system was configured.

❖ **Edit**

- Edit Retention Category (Category level): displays the Create or Edit Retention Category Page (page 8-42).
- Edit Disposition (Category level): displays the Disposition Instructions Page (page 14-24).
- Edit Review (Category level and Folder level): displays the Edit Review information screen. See Records Manager DoD Edition System Maintenance Guide for details.
- Edit Series (Series level): displays the Create or Edit Series Page (page 8-39).
- Move (all): displays the Select Retention Series, Folder or Category Screen (page 8-41).
- Hide (Series level): displays a prompt screen for you to indicate why the object is being hidden.
- Freeze/Unfreeze (Folder level): Toggles between freeze or unfreeze for a records folder.

❖ **Delete**

- Delete Category (Category level): removes a category.
- Delete Folder (Folder level): removes a folder
- Delete Tree (all): recursively deletes an object and its children.
- Delete Series (Series level): deletes a series.

❖ **Create**

- Create Records Folder (Category level and Folder level): displays the Create or Edit Records Folder Page (page 8-49).
- Create Record (Category level and Folder level): displays the Content Checkin Form.
- Create Series (Series level): displays the Create or Edit Series Page (page 8-39).
- Create Retention Category (Series level): displays the Create or Edit Retention Category Page (page 8-42).

❖ **Change View**

- Thumbnail: presents a icon-based ‘thumbnail’ view.
- Headline: presents a horizontal, ‘headline’ view.

In addition, the following options are available on the individual item Action menus on the Folder page as well as on the Table menu on the Folder level:

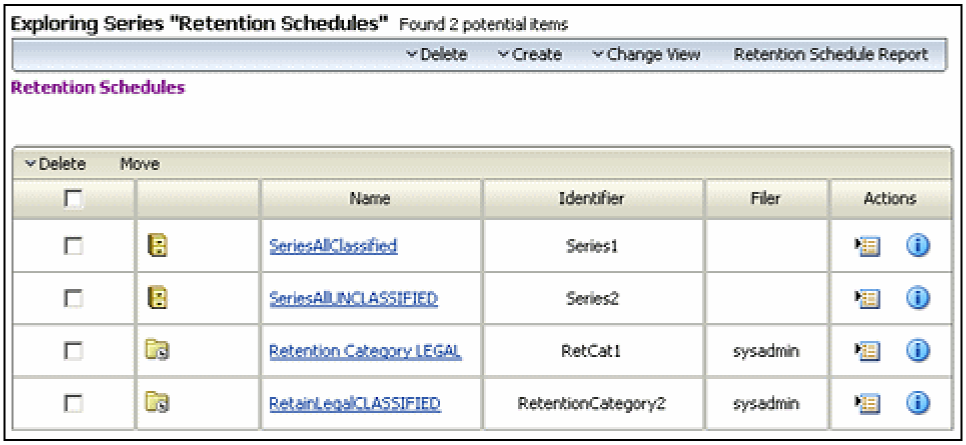
❖ **Trigger Dates**

- Mark reviewed: Marks a records folder a reviewed.
- Mark recursive: Marks all child objects as reviewed.
- Cancel: Marks the folder as cancelled, making it obsolete.
- Expire: expires all records in a folder, making records obsolete.
- Obsolete: marks records and the folder as obsolete. This toggles to Undo Obsolete if a folder becomes obsolete due to specific actions.
- Rescind: rescinds a records folder and the records therein.
- Undo Cutoff (Table menu only): reverses the cutoff status of a folder.
- Undo Obsolete (Table menu only): marks records and the folder as not obsolete.

Main Root or Series Level

The main root node is considered the retention schedule series node. At the series level, you can create a series or retention category:

Figure 8-5 Browsing Series page

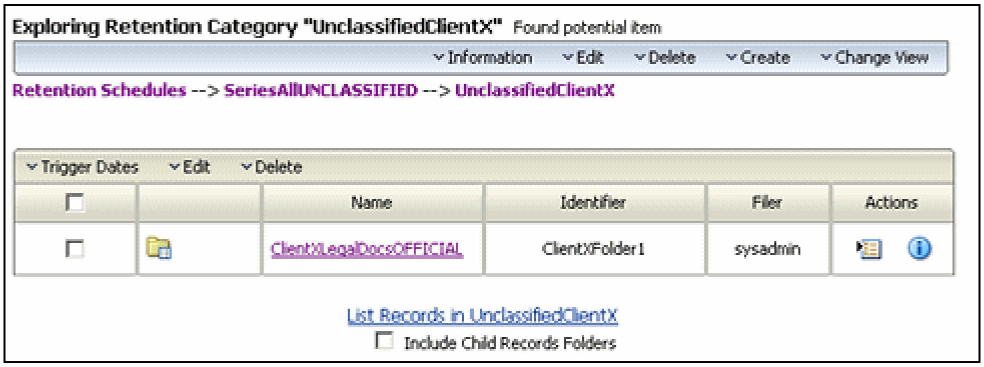

Exploring Series "Retention Schedules" Found 2 potential items
Delete
Create
Change View
Retention Schedule Report
Retention Schedules
Delete
Move

□		Name	Identifier	Filer	Actions
□		SeriesAllClassified	Series1		
□		SeriesAllUNCLASSIFIED	Series2		
□		Retention Category LEGAL	RetCat1	sysadmin	
□		RetainLegalCLASSIFIED	RetentionCategory2	sysadmin	

Retention Category Level

At the retention category level, you can create records folders, records, or non-record content. The Exploring Retention Category page provides a link that displays items filed within the category, including an option to also show items filed within any child folders.

Figure 8-6 Browsing a retention category



Exploring Retention Category "UnclassifiedClientX" Found potential item

Retention Schedules --> SeriesAllUNCLASSIFIED --> UnclassifiedClientX

□		Name	Identifier	Filer	Actions
□		ClientXLegalDocsOFFICIAL	ClientXFolder1	sysadmin	

List Records in UnclassifiedClientX

□ Include Child Records Folders

If you create a record at the category level in the example above, the record is filed into the series and not in the folder. Also note, that the actions that are displayed vary based on if the retention category is for records or non-record content items.

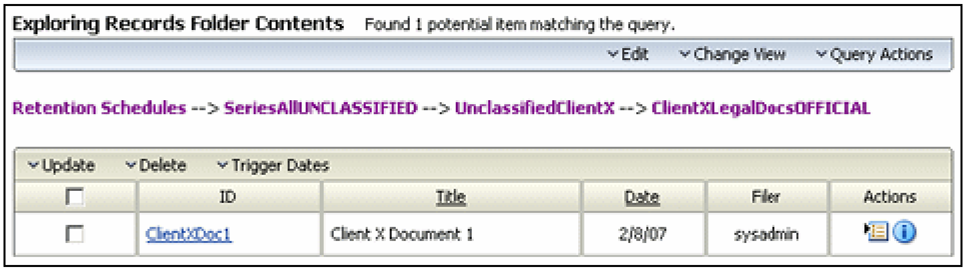
Note: The link on this page is called **List Content Items** for categories that have been marked as non-record categories. See Is Non-Record Category check box (page 8-45), and **List Records** link for "normal" retention categories.

Records Folder Level

At the records folder level, you can create records folders or records. The Exploring Records Folder page provides a link that displays items filed within the records folder, including an option to also show items filed within any child folders.

Note: Records folders contain records only. They do not contain non-record content items.

Figure 8-7 Browsing record folder content



Exploring Records Folder Contents Found 1 potential item matching the query.

Retention Schedules --> SeriesAllUNCLASSIFIED --> UnclassifiedClientX --> ClientXLegalDocsOFFICIAL

□	ID	Title	Date	Filer	Actions
□	ClientXDoc1	Client X Document 1	2/8/07	sysadmin	

After you create your retention schedule, you can generate a retention schedule report on the entire retention schedule from the Configure Root Nodes page (see Configuring the Root Nodes (page 7-12)), or on any portion of the plan from numerous locations. For more information about generating retention schedule reports, see the *Records Manager DoD Edition User Guide*.

USING A SERIES

A series is an optional feature for organizing records and non-record content items. If an organization has a multitude of retention categories, setting up series can assist with managing the view of the retention schedule hierarchies. You can nest series within each other. Series are also useful for creating work-in-progress retention schedules because series can be hidden from users, which prevents records or non-record content item users from filing any records into the hidden series.

This section covers the following topics:

- Managing Series (page 8-15)
- See also Series Interface Screens (page 8-38) at the end of this chapter

Managing Series

Permissions: The appropriate records management rights are required to work with series. There are separate rights for reading (viewing), creating, deleting, moving, editing, and hiding/unhiding series. The predefined ‘rma’ and ‘rmaprivileged’ roles can only read (view) series. The predefined ‘rmaadmin’ role can also perform any of the other series-related tasks.

The following tasks are involved in managing series:

- Creating or Editing a Series (page 8-16)
- Viewing Series Information (page 8-17)
- Hiding and Unhiding a Series (page 8-17)
- Moving a Series (page 8-18)
- Deleting a Series (page 8-19)
- Deleting a Tree (Recursive Delete) (page 8-20)

Creating or Editing a Series

You can create nested series; that is, a series within a series.

Permissions: The Series.Create right is required to perform this action. This right is assigned by default to the 'rmaadmin' role.

1. Open the **Browse Content** tray and click the **Retention Schedules** link.

   The Exploring Series "Retention Schedule" page is displayed.

2. Navigate to the location in which to create the series.
3. Click **Create—Series** from the **Actions** list in an existing series or from the Page menu.

   The Create or Edit Series Page (page 8-39) is displayed.

4. Enter an identifier for the series in the **Series Identifier** text box.
5. Enter a name for the series in the **Series Name** text box.
6. Click **Create**. The series is displayed in both the Browse Content tray area and in the Retention Schedule list.

Use the following procedure to edit the name for the series. You can edit any information except the series identifier.

Permissions: The Series.Edit right is required to edit a series. This right is assigned by default to the 'rmaadmin' role.

1. Open the **Browse Content** tray, and click the **Retention Schedules** link.

   The Exploring Series "Retention Schedule" page is displayed.

2. In the **Actions** list for the series to edit, click **Edit—Edit Series**.

   The Create or Edit Series Page (page 8-39) is displayed.

3. Enter any changes to the value in the **Series Name** box, and click **Submit Update**. A message is displayed saying that the series was updated successfully.
4. Click **OK**.

You may also edit a series from the Series Information Page (page 8-40) by clicking **Edit** on the Page menu.

Viewing Series Information

Permissions: The Series.Read right is required to perform this action. This right is assigned by default to all roles.

1. Open the **Browse Content** tray and click the **Retention Schedules** link.

   The Exploring Series “Retention Schedule” page is displayed.

2. Navigate to the series to view information.

3. In the row for the series, do one of the following:

   - Click the Info icon (ℹ).
   - Click the Actions icon (☰), and choose **Information—Series** from the popup.

   The Series Information Page (page 8-40) is displayed. This page shows relevant information about the selected series.

4. Click **OK** when you finish viewing information.

Hiding and Unhiding a Series

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, you can unhide the series.

Permissions: The Series.Hide/Unhide right is required to perform these actions. This right is assigned by default to the ‘rmaadmin’ role.

1. Open the **Browse Content** tray and click the **Retention Schedules** link.

   The Exploring Series “Retention Schedule” page is displayed.

2. Navigate to the series to hide.

3. Choose **Edit—Hide** from the Item **Action** popup menu.

4. You are prompted to enter a reason for the action. If desired, enter a reason, and click **OK** to confirm. If you do not want to enter a reason, leave the text box empty, and click **OK**. If you click **Cancel**, the entire action is aborted.

   If you confirmed the action, the series icon is now semi-transparent (▤) to indicate it is hidden.

Follow this procedure to unhide the series:

1. Open the **Browse Content** tray and click the **Retention Schedules** link.

   The Exploring Series “Retention Schedule” page is displayed.

2. Navigate to the series to unhide.
3. Choose **Edit—Hide** from the Item **Action** popup menu.
4. You are prompted to enter a reason for the action. If desired, enter a reason, and click **OK** to confirm. If you do not want to enter a reason, leave the text box empty, and click **OK**. If you click **Cancel**, the entire action is aborted.

   If you confirmed the action, the series icon is no longer semi-transparent to indicate it is not hidden.

Moving a Series

All child series, categories, records folders and records and non-record content items move with the parent series.

Permissions: The Series.Move right is required to perform this action. This right is assigned by default to the ‘rmaadmin’ role.

1. Open the **Browse Content** tray and click the **Retention Schedules** link.

   The Exploring Series “Retention Schedule” page is displayed.

2. Navigate to the series to move.
3. Choose **Edit—Move** from the Item **Action** popup menu.

   The Select Retention Series, Folder or Category Screen (page 8-41) is displayed.

4. Click to expand the tree, and click on the series to move to. The location field populates with the new location.
5. Click **OK**. The Exploring Series page displays the series in its new location.

To move multiple series, complete the following steps:

1. Open the **Browse Content** tray and click the **Retention Schedules** link.

   The Exploring Series “Retention Schedule” page is displayed.

2. Click the **Select** check boxes for each series to move.
3. Choose **Move** from the Table **Actions** list. The Select Retention Series screen is displayed.

4. Click to expand the tree, and click on the series or category to which to move the category. The location field populates with the new location.

5. Click **OK**. The Exploring Series page and Browse Content area displays the series in its new location.

Deleting a Series

A series must be empty before you can delete it using the Delete command. An empty series means that it does not contain any child objects, such as series, categories, records folders, and records or non-record content items. Be sure to move or delete records, non-record content items, records folders, categories, and any nested series from the series to delete.

Tech Tip: To delete multiple series, enable the **Select** check boxes for the series and choose **Delete** from the Table **Actions** list. To delete a series and its child series and categories, and records folders with one command, do a recursive delete with the Recursive Delete command. With either delete command, there must not be any records filed in a records folder or category. For more information, see Deleting a Tree (Recursive Delete) (page 8-20).

Permissions: The Series.Delete right is required to perform this action. This right is assigned by default to the ‘rmaadmin’ role.

1. Open the **Browse Content** tray and click the **Retention Schedules** link.

   The Exploring Series “Retention Schedule” page is displayed.

2. Navigate to the series to delete.

3. Choose **Delete—Series** from the Item **Action** popup menu.

4. You are prompted to confirm the delete. Click **OK** to delete the series, or **Cancel** to cancel the delete action.

5. You are prompted to enter a reason for the action. If desired, enter a reason, and click **OK** to confirm. If you do not want to enter a reason, leave the text box empty, and click **OK**. If you click **Cancel**, the entire action is aborted.

   If you confirmed the action, the series is deleted from the retention schedule.

To delete multiple series, complete the following steps:

1. Open the **Browse Content** tray on the left, and click the **Retention Schedules** link. The Exploring Series “Retention Schedule” page is displayed.

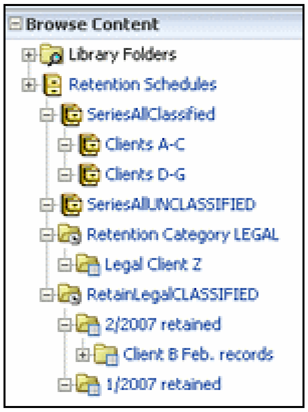
2. Click the check boxes for each series to delete.
3. From the Table **Actions** list, click **Delete**.
4. You are prompted to confirm the delete. Click **OK** to delete the series, or **Cancel** to cancel the delete action.
5. You are prompted to enter a reason for the action. If desired, enter a reason, and click **OK** to confirm. If you do not want to enter a reason, leave the text box empty, and click **OK**. If you click **Cancel**, the entire action is aborted.

   If you confirmed the action, the series are deleted from the retention schedule.

Deleting a Tree (Recursive Delete)

Use this procedure to delete a series, category, or records folder and all of its children, provided there are no items filed within a category or records filed within a records folder. The recursive delete feature is useful for quickly eliminating obsolete sections of retention schedules. Otherwise, you have to manually delete each records folder, category, and series from the bottom of a retention schedule hierarchy upwards.

Figure 8-8 Nested retention schedule objects



This illustrates nested series and records folders. If you choose the Delete Tree command on “RetainLegalCLASSIFIED” shown above, the category and its children “2/2007 retained,” “Client B Feb. records,” and “1/2007 retained” are deleted, provided there are not any items contained within. If the system encounters a category or records folder that contains items, it stops at that point, gives a message stating a category or records folder contains items, and refrains from deleting any further children. At that point, manual intervention is required. Move the items to another location or delete the items if they are not permanent and no longer needed, and try the recursive delete again.

Caution: Be sure you want to delete everything under and including the object you are deleting because you cannot undo a delete. To target a specific object to delete without the delete cascading down to child objects, use the Delete command instead.

Permissions: Delete rights for all retention schedule components in the tree are required. For example, if the tree consists of series and categories, Series.Delete and Category.Delete rights are required. If it also includes records folders, Folder.Delete rights are also required.

1. Open the **Browse Content** tray and click the **Retention Schedules** link.

   The Exploring Series "Retention Schedule" page is displayed.

2. Navigate to the series, retention category, or records folder to delete.
3. Select **Delete—Delete Tree** from the Item **Action** popup menu.
4. You are prompted to confirm the delete. Click **OK** to delete, or **Cancel** to cancel the delete.
5. You are prompted to enter a reason for the action. If desired, enter a reason, and click **OK** to confirm. If you do not want to enter a reason, leave the text box empty, and click **OK**. If you click **Cancel**, the entire action is aborted.

   If you confirmed the action, the series tree is deleted from the retention schedule.

Retention Categories

A retention category is a retention schedule object that has associated security settings and disposition instructions defined. Retention categories cannot be nested within other retention categories.

This section covers the following topics:

- Managing Retention Categories (page 8-22)
- Retention Category Examples (page 8-27)
- See also Category Interface Screens (page 8-42) at the end of this chapter

Note: If ACLs are on the retention category, the records user must also be on the ACL to view or access the retention category.

After you are at the category level, you can create records folders, records, or non-record content items.

Managing Retention Categories

The following tasks are involved in managing retention categories:

- Creating or Editing a Retention Category (page 8-22)
- Viewing Retention Category Information (page 8-24)
- Viewing Category Metadata History (page 8-25)
- Moving a Retention Category (page 8-26)
- Deleting a Retention Category (page 8-26)

Permissions: The appropriate records management rights are required to work with retention categories. There are separate rights for reading (viewing), creating, deleting, moving, and editing categories. The predefined ‘rma’ and ‘rmaprivileged’ roles can only read (view) categories. The predefined ‘rmaadmin’ role can also perform any of the other category-related tasks.

Creating or Editing a Retention Category

A retention category can contain records folders, records, or non-record content. You can create retention categories at the root node level, or within a series.

Permissions: The Category.Create right is required to perform this action. This right is assigned by default to the ‘rmaadmin’ role.

1. Open the **Browse Content** tray and click the **Retention Schedules** link. The Exploring Series “Retention Schedule” page is displayed.
2. Click **Create—Create Retention Category** from the Page menu. You can also navigate to a listed series and click **Create—Create Retention Category** from the Item **Actions** list.

   The Create or Edit Retention Category Page (page 8-42) is displayed.
3. (Optional) If you do not want to accept the default security group (RecordsGroup) select a group from the **Security Group** list. The **Default Content Server security for Categories, Folders, and Triggers** check box must be enabled on the Configure Records Management Page (page 7-2).
4. (Optional) If Accounts are enabled, indicate the associated account for the category in the **Account** box.

5. (Optional) If your organization uses the default Content Server security 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 in the **Retention Category Identifier** box.
7. Enter a name for the category in the **Retention Category Name** box.
8. Enter a description of up to 1000 characters in the **Retention Category Description** box.
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. If this is a retention category used to contain non-record content items, select the Is **Non-Records Category** box. If this is selected, the **Permanent** box is grayed out, indicating that non-record content items cannot be designated as permanent.
11. (Optional) If the retention category is a record retention category and will contain permanent records, then select the **Permanent** check box.
12. If the content is not allowed to be deleted, select the **Disallow Content Delete** checkbox.
13. (Optional) If the retention category is to contain records or non-record content for review, and you want all folders and records to inherit the subject to review status, then do the following:
    a. Select the **Subject to Review** check box.
    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.
    c. Enter an integer value for the number of review periods in the **Review Period** text box.
    d. Select the defined period from the **Review Period** list.
14. (Optional) If your organization uses access control lists (ACLs), then assign group permissions to the category:
    a. To assign group permissions, click **Select** by the **Group Permissions** box. The Select Alias screen is displayed.
    b. 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 to

set permissions for, and click **OK**. The alias and its permissions display in the Group Permissions text box of the Create Retention Category page.

15. (Optional) If your organization uses access control lists (ACLs), then assign user permissions to the category:

    a. By the **User Permissions** box, click **Select**. The Select User screen is displayed.

    b. 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 to set permissions for, and click **OK**. The user and their permissions display in the User Permissions text box of the Create Retention Category page.

16. Click **Create**. The Dispositions Instructions page is displayed. You can create a disposition rule at this time. If you do not want to create a disposition at this time, just click **Submit Update**.

    For more detailed instructions about disposition rules and disposition examples, see Chapter 14 (*Defining Disposition Instructions)*.

Use this procedure to edit an existing retention category.

Permissions: The Category.Edit right is required to perform this action. This right is assigned by default to the ‘rmaadmin’ role.

1. Open the **Browse Content** tray and click the **Retention Schedules** link.

   The Exploring Series “Retention Schedule” page is displayed.

2. Navigate to the retention category to edit.

3. Select **Edit—Edit Retention Category** from the Item **Actions** popup menu.

   The Create or Edit Retention Category Page (page 8-42) page is displayed.

4. Enter your changes to the available fields.

5. Click **Submit Update**. The successfully updated retention category message is displayed.

6. Click **OK**. The Exploring Series “Retention Schedule” page is displayed at the location to which you navigated.

Viewing Retention Category Information

Permissions: The Category.Read right is required to perform this action. All predefined roles this right.

1. Open the **Browse Content** tray and click the **Retention Schedules** link.

   The Exploring Series “Retention Schedule” page is displayed.

2. Navigate to the retention category to view information.

3. In the row for the category, do one of the following:

   - Click the Info icon (ⓘ).
   - Choose **Information—Retention Category Information** from the Item **Actions** popup menu.

   The Retention Category Information Page (page 8-48) is displayed. This page shows relevant information about the selected retention category.

4. Click **OK** when done.

Viewing Category Metadata History

Use this procedure to view the metadata history of a retention category—that is, a list of all changes that have been made to the editable category properties.

Permissions: The Category.Edit right is required to perform this action. This right is assigned by default to the ‘rmaadmin’ role.

1. Open the **Browse Content** tray and click the **Retention Schedules** link.

   The Exploring Series “Retention Schedule” page is displayed.

2. Navigate to the appropriate retention category.

3. Select **Information—Metadata History** from the Item **Actions** popup menu.

   The Metadata History Page (page 8-48) is displayed, 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

4. Click **OK** when you finish.

You can also view the metadata history from the Retention Category Information Page (page 8-48) by choosing **Information—Metadata History** from the Page menu.

Moving a Retention Category

You can move a retention category to another series or to the root node retention schedule level.

Permissions: The Category.Move right is required to perform this action. This right is assigned by default to the 'rmaadmin' role.

1. Open the **Browse Content** tray and click the **Retention Schedules** link.

   The Exploring Series "Retention Schedule" page is displayed.
2. Navigate to the retention category to move.
3. Select **Edit—Move** from the Item **Actions** popup menu.

   The Select Retention Series, Folder or Category Screen (page 8-41) is displayed.
4. Click to expand the tree, and click on the series to which to move the category. The location field populates with the new location.
5. Click **OK**. The Exploring Series page and Browse Content area display the retention category in its new location.

Deleting a Retention Category

Use this procedure to delete a retention category. A retention category must be empty before you can delete it using the Delete command. To empty a retention category, you must move or delete any child records folders and records or non-record content items.

Tech Tip: To delete multiple categories, enable the **Select** check boxes for the categories and choose **Delete** from the Table **Actions** list. To delete a retention category and its child categories and records folders with one command, do a recursive delete with the **Delete Tree** command. For more information, see *Deleting a Tree (Recursive Delete)* (page 8-20).

Permissions: The Category.Delete right is required to perform this action. This right is assigned by default to the 'rmaadmin' role. Delete permission (D) for the RecordsGroup security group is also required.

1. Open the **Browse Content** tray and click the **Retention Schedules** link.

   The Exploring Series "Retention Schedule" page is displayed.
2. Navigate to the retention category to delete.
3. Choose **Delete—Delete Category** from the Item Actions popup menu.

4. You are prompted to confirm the delete. Click **OK** to delete the category, or **Cancel** to cancel the delete.

5. You are prompted to enter a reason for the action. If desired, enter a reason, and click **OK** to confirm. If you do not want to enter a reason, leave the text box empty, and click **OK**. If you click **Cancel**, the entire action is aborted.

   If you confirmed the action, the retention category is deleted from the retention schedule.

Retention Category Examples

The following examples demonstrate the use of retention categories:

- Creating a Permanent Retention Category (page 8-27)
- Creating a Retention Category that is Subject to Review (page 8-28)
- Creating a Non-Permanent Retention Category (page 8-29)

Creating a Permanent Retention Category

This example demonstrates creating a permanent retention category with an accession disposition schedule. Permanent records usually have an accession disposition action to a Federal Records Center. Although dispositions are the subject of Chapter 14 (*Defining Disposition Instructions)*, quick disposition instructions are previewed in context within the examples.

1. Open the **Browse Content** tray and click the **Retention Schedules** link.

   The Exploring Series “Retention Schedule” page is displayed.

2. Select **Create—Create Retention Category** from the Page menu.

   The Create or Edit Retention Category Page (page 8-42) is displayed.

3. Enter `RCP-101` in the **Retention Category Identifier** box.

4. Enter `Permanent Category 101` in the **Retention Category Name** box.

5. Enter a description of up to 1,000 characters in the **Retention Category Description** box. For this example, type `RCP-101`.

6. (Required for U.S. Government Agencies) Enter the code of the authority for the disposition in the **Disposition Authority** box. For this example, type `RCP-101`.

7. Select the **Permanent** check box.

8. Click **Create**.

   The Disposition Instructions Page (page 14-24) is displayed.

   a. Click **Add**. The Disposition Rule Screen (page 14-25) is displayed.
   b. Leave **After** (**Triggering Event**) as "Retention Period Cutoff."
   c. Enter `5 Calendar Years` for **Wait For** (the **Retention Period**).
   d. In the **Do** (**Disposition Action**) list, select **Accession**.
   e. In the **To Location** (**Destination Location**) box, type `NARA`.
   f. Click **OK**.
   g. The Disposition Rule Screen (page 14-25) is displayed again.

9. Click **Submit Update**.
10. Click **OK**.

Creating a Retention Category that is Subject to Review

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. Open the **Browse Content** tray and click the **Retention Schedules** link.

   The Exploring Series "Retention Schedule" page is displayed.

2. Select **Create—Create Retention Category** from the Page menu.

   The Create or Edit Retention Category Page (page 8-42) is displayed.

3. Enter `RCV-101` in the **Retention Category Identifier** box.
4. Enter `Operational for Review` in the **Retention Category Name** box.
5. Enter a description of up to 1000 characters in the **Retention Category Description** box. For this example, type `RCV-101`.
6. (Required for U.S. Government Agencies) Enter the code of the authority for the disposition in the **Disposition Authority** box. For this example, type `RCV-101`.
7. Do ***not*** select the **Permanent** check box.
8. Select the **Subject to Review** check box.
9. Specify a **Reviewer** and a **Review Period**.
10. Click **Create**.

    The Disposition Instructions Page (page 14-24) is displayed.

   a. Click **Add**. The Disposition Rule Screen (page 14-25) is displayed.
   b. Leave the **After** (**Triggering Event**) as “Retention Period Cutoff.”
   c. Enter `3 Calendar Months` as **Wait For** (the **Retention Period**).
   d. In the **Do** (**Disposition Action**) list, select **Archive**.
   e. Click **OK**.

11. Click **Submit Update**.
12. Click **OK**.

Creating a Non-Permanent Retention Category

This example demonstrates creating a retention category to contain content items records that are not permanent. A temporary retention category typically constitutes the majority of records in a records management system, and are usually slated for destruction. This example creates a destruction (destroy) disposition action for the temporary retention category.

To create a temporary retention category, complete the following steps:

1. Open the **Browse Content** tray and click the **Retention Schedules** link.

   The Exploring Series “Retention Schedule” page is displayed.

2. Select **Create—Create Retention Category** from the Page menu.

   The Create or Edit Retention Category Page (page 8-42) is displayed.

3. Enter `RCT-101` in the **Retention Category Identifier** box.
4. Enter a name for the retention category in the **Retention Category Name** box.
5. Enter a description of up to 1000 characters in the **Retention Category Description** box. For this example, type `RCT-101`.
6. (Required for U.S. Government Agencies) Enter the code of the authority for the disposition in the **Disposition Authority** box. For this example, type `RCT-101`.
7. Do ***not*** select the **Permanent** check box.
8. Click **Create**.

   The Disposition Instructions Page (page 14-24) is displayed.

   a. Click **Add**. The Disposition Rule Screen (page 14-25) is displayed.
   b. Leave **After** (the **Triggering Event**) as “Retention Period Cutoff.”
   c. Enter `1 Calendar Years` as **Wait For** (the **Retention Period**).

   d. In the **Do** (**Disposition Action**) list, select **Destroy**.
   e. Click **OK**.

9. Click **Submit Update**.
10. Click **OK**.

Records Folders

Note: Records folders can contain only records. They cannot contain non-record content items.

Records differ from documents in the content server in that records have different metadata, and records are associated with a disposition life cycle. A records folder organizes similar records within a retention category. A retention category can have multiple records folders, and records folders can be nested within other records folders. Records folders inherit disposition rules from their parent records folder or category. A records folder can also have its own disposition rule or rules unique to a specific records folder.

This section covers the following topics:

- About Records Folders (page 8-30)
- Managing Records Folders (page 8-31)
- Folder Examples (page 8-36)
- See also Folders Interface Screens (page 8-49) at the end of this chapter

About Records Folders

A record folder can inherit security settings from a category, or have its own security settings. Supplemental markings can also be set on a records folder and users to further secure the folder above and beyond all other security mechanisms. In addition to inheriting security settings and disposition rules, folders also inherit record review information from their parent category. If a folder is inheriting review information, it is indicated on the Records Folder Information page.

The review information that takes precedence is at the lowest node (the shortest review period prevails), such as in the case of nested folders. You can override record review information at the record folder level. For example, you can specify a different reviewer or review period cycle; however, you cannot specify a folder within a retention category that is subject to review as a folder that is not subject to review. If you do not want a records folder to be reviewed, you must create the folder in a non-subject to review category.

Permissions: The appropriate records management rights to work with records folders are required. Separate rights are required for reading (viewing), creating, deleting, opening/ closing, editing, moving, and freezing/unfreezing folders. The predefined 'rma' role can only read (view) records folders. The predefined 'rmaprivileged' role can read, create, edit, and move folders. The predefined 'rmaadmin' role can perform all folder-related tasks.

Records folder objects are unique from other retention schedule objects in that the records folders for temporary records are destroyed with the records. The records folders also have a life cycle that parallels that of its records. Records administrators must recreate records folders on a regular basis, whereas this is not typically true of records series or categories in the retention schedule.

Managing Records Folders

The following tasks are involved in managing folders:

- Creating a Records Folder (page 8-31)
- Editing a Records Folder (page 8-34)
- Moving a Records Folder (page 8-35)
- Deleting a Records Folder (page 8-35)

For details about viewing folder information, see the *Records Manager DoD Edition System Maintenance Guide.*

Creating a Records Folder

Use this procedure to create a records folder within a retention category, or as a child folder of another records folder.

Permissions: The Folder.Create right is required to perform this action. This right is assigned by default to the 'rmaprivileged' and 'rmaadmin' roles.

Prerequisites:

- Creating or Editing a Retention Category (page 8-22)
- Chapter 10 (*Configuring Time Periods)* (for cycling records for review).

❖ Creating or Editing a Supplemental Marking (page 6-7) (optional)

This procedure also assumes you have your security configured and have assigned rights to users.

1. Open the retention category or records folder in which to create a records folder.
2. From the **Actions** list, click **Create—Records Folder**.

   The Create or Edit Records Folder Page (page 8-49) is displayed.
3. (Optional) If you do not want to accept the **RecordsGroup** option as your default security group, then select the group from the **Security Group** list.
4. (Optional) If your organization uses accounts in your security model, then select the account associated to the folder from the **Account** list. For more information about accounts, see the Administration documentation for Content Server.
5. (Optional) To change the filer (referred to as “author” in standard Content Server) of the records folder from the default, select the user in the **Filer** field.
6. Enter a unique identifier in the **Records Folder Identifier** box.
7. Enter a name for the records folder in the **Records Folder Name** box.
8. (Optional) Enter a description of the folder in the **Records Folder Description** box.
9. (Optional) If the records folder is going to contain records that are subject to review:
   a. Select the **Subject to Review** check box.
   b. Select a **Reviewer** for notifications to override the system default set in the Configure Records Management Page (page 7-2) page.

Permissions: The reviewer you select must have the Folder.EditReview right. Without that right, the reviewer cannot mark a records folder as reviewed.

   c. Enter the number and select type of period in the **Review Period** fields.

Note: If the category of a records folder is defined as subject to review, and a child records folder does not have its own review information defined, then the records folder inherits the review information from its category or its parent records folder. For further details, see Attribute Inheritance (page 8-8).

10. (Optional) If the records folder has external characteristics:
    a. If the folder is external, select the **External** check box.
    b. (Required if External selected) Enter an external physical location for the records folder in the **External Location** box, if applicable.

   c. (Optional) Enter a physical container code or description for the records folder in the **Container** text box, if applicable.

11. (Optional) To assign supplemental markings to the folder, select one or more markings from the **Supplemental Markings** list.

Permissions: Even if a user or group has permission to access a records folder, supplemental markings can still restrict records folder access. For more information, see Supplemental Markings Details (page 6-3).

12. (Optional, for ACL-enabled implementations) Set up ACL access at the alias level:
    a. To assign access at the group (user alias) level, click **Select**. The Select Alias screen is displayed.
    b. Type the alias name or select it in the alias name list box. You must have set up aliases for users in Content Server's User Admin utility. For more information, see the administrator documentation for Content Server.
    c. Select the check boxes for the permissions (Read, Write, Delete, Admin) to the records folder.
    d. Click **Add to List**. The alias and permissions are displayed in the Add to List text box.
    e. Repeat for each alias as necessary. When you are done assigning alias access, click **OK**. Each alias and its permissions are displayed in the Group Permissions box.
13. (Optional, for ACL-enabled implementations) Set up ACL access at the specific user level:
    a. To assign access at the user level, click **Select** next to the **Group Permissions** text box. The Select Alias screen is displayed.
    b. Type the user name or select it in the user name list box. You must have set up your system users in Content Server's User Admin utility. For more information, see the administrator documentation for Content Server.
    c. Select the check boxes for the user permissions (Read, Write, Delete, Admin) to the records folder.
    d. Click **Add to List**. Repeat for each user as necessary. The users and their permissions are displayed in the **Add to List** text box.
    e. When you are done assigning user access, click **OK**. Each user and their permissions are displayed in the **User Permissions** text box.

Note: Using aliases provides more efficient management of group ACL because the users can be aliased to a group. This abstracts the user name to an alias, so that only the alias name needs to be maintained, rather than assigning individual user permissions and access. For more information about aliases, see the administrator documentation for Content Server. Set ACL at the user level if a user has unique access requirements that cannot be accommodated by a common alias group.

14. Click **Create**. The records folder is displayed in the exploring retention category or records folder page.

Editing a Records Folder

Occasions on which you would edit a records folder include updating:

- specific user access for ACL if you do not use alias/group permission
- a reason for freezing a records folder
- activation or expiration dates for internal record content
- elaborating on or editing a folder description
- the physical locations and containers for the physical counterpart of electronic records as the records progress through their life cycle and are transferred to other locations.

Permissions: To edit a records folder that you authored, you must have the Folder.EditIfAuthor right. This right is assigned by default to the ‘rmaprivileged’ role. To edit a records folder that you did not author, you must have the Folder.Edit right. This right is assigned by default to the ‘rmaadmin’ role.

1. Open the **Browse Content** tray, and click the **Retention Schedules** link.

   The Exploring Series “Retention Schedule” page is displayed.

2. Navigate to the records folder to edit.
3. Select **Edit—Records Folder** from the **Actions** popup menu.

   The Create or Edit Records Folder Page (page 8-49) is displayed.

4. Make your desired changes to the available fields.
5. Click **Submit Update**. The successfully updated folder message and your edits are displayed on the Records Folder Information Page (page 8-58). Click **OK**.

Moving a Records Folder

Use this procedure to move a records folder to a retention category or to another folder.

Permissions: The Folder.Move right is required to perform this action. This right is assigned by default to the ‘rmaprivileged’ and ‘rmaadmin’ roles.

1. Open the **Browse Content** tray, and click the **Retention Schedules** link.

   The Exploring Series “Retention Schedule” page is displayed.

2. Navigate to the records folder to move.

3. Choose **Edit—Move** from the Item Action popup menu.

   The Select Retention Series, Folder or Category Screen (page 8-41) is displayed.

4. Click to expand the tree, and drill down in the hierarchy until you reach the category or folder where the records folder will be moved. The location field populates with the new location.

5. Click **OK**. The Exploring Category or Exploring Folder page and Browse Content area display the records folder in its new location.

Deleting a Records Folder

A records folder must be empty, that is, not contain any child records folders or records before you can delete the records folder using the Delete command.

Caution: If a records folder has its own disposition rule or rules defined for it, deleting the records folder deletes the disposition rule from the record category. To prevent the rule from being deleted, remove the association to the specific records folder. This is discussed in more detail in the *Records Manager DoD Edition System Maintenance Guide.*

Tech Tip: To delete multiple records folders, enable the **Select** check boxes for the folders and choose **Delete** from the Table **Actions** list. To delete a records folders and its child records folders with one command, do a recursive delete using the Delete Tree command. The folder must be devoid of records to use the Delete Tree command. For more information, see Deleting a Tree (Recursive Delete) (page 8-20).

Permissions: The Folder.Delete right is required to delete a records folder. This right is assigned by default to the ‘rmaadmin’ role.

1. Open the retention category that contains the records folder to delete.

2. Navigate to the records folder to delete.

3. Click **Delete—Delete Records Folder** from the Item **Actions** popup menu.

4. You are prompted to confirm the delete. Click **OK** to delete, or **Cancel** to cancel the delete.

5. You are prompted to enter a reason for the action. If desired, enter a reason, and click **OK** to confirm. If you do not want to enter a reason, leave the text box empty, and click **OK**. If you click **Cancel**, the entire action is aborted.

   If you confirmed the action, the records folder is deleted from the retention schedule.

Folder Examples

The following examples demonstrate folder management tasks:

- Creating a Records Folder That is Subject to Review (page 8-36)
- Creating an External Records Folder (page 8-37)
- Creating Records Folders Subject to Recurring Audit Triggers (page 8-37)

Creating a Records Folder That is Subject to Review

This example records folder has a three month review cycle. Editing a review cycle requires accessing a special edit page. For further information, see the *Records Manager DoD Edition System Maintenance Guide*.

1. Open the retention category or records folder where you'll create a records folder.

2. From the **Actions** list, click **Create Records Folder**.

   The Create or Edit Records Folder Page (page 8-49) is displayed.

3. Enter `RFV-101` in the **Records Folder Identifier** box.

4. Enter `RFV-101` in the **Records Folder Name** box.

5. Select the **Subject to Review** check box.

6. Select a **Reviewer** to receive e-mail notifications when it is time to review the records folder.

7. Enter `3 Months` as the **Review Period**.

8. Click **Create**. The records folder displays in the Exploring Retention Cateogory page. Click the Info icon for the new records folder. The Records Folder Information page displays "Subject to Review: Yes" and displays the corresponding Review Period.

Any inherited review information from a parent records folder or from the retention category is also given.

Creating an External Records Folder

This example demonstrates creating a records folder to track external records contained externally in physical records folders. For information about filing records into an external records folder, see the *Records Manager DoD Edition User Guide*.

1. Open the retention category or records folder where you'll create a records folder.
2. From the **Actions** list, click **Create Records Folder**.

   The Create or Edit Records Folder Page (page 8-49) is displayed.
3. Enter `RFE-101` in the **Records Folder Identifier** box.
4. Enter `RFE-101` in the **Records Folder Name** box.
5. Select the **External** check box.
6. Enter `Warehouse A` in the **External Location** box.
7. In the **External Container** box, enter `File Cabinet Row xy.`
8. Click **Create**. The records folder displays in the Exploring Retention Schedules page. Click the Info icon for the new records folder. The Records Folder Information page displays "External: Yes" and displays the corresponding external fields, which in this example is "External Location: Warehouse A" and "External Container: File Cabinet Row xy."

Creating Records Folders Subject to Recurring Audit Triggers

This example demonstrates creating a records folder that is subject to the recurring audit trigger. For more information about the built-in recurring audit trigger, see Trigger Overview (page 9-2). The Audit Periods must already be defined in Content Server's Configuration Manager utility. For further information about configuring audit period lists, see the *Records Manager DoD Edition Installation Guide*.

To create an audited records folder, complete the following steps:

1. Open the retention category or records folder where you'll create a records folder.
2. From the **Actions** list, click **Create Records Folder**.

   The Create or Edit Records Folder Page (page 8-49) is displayed.

3. Enter `RFA-101` in the **Records Folder Identifier** box.
4. Enter `RFA-101` in the **Records Folder Name** box.
5. Select the **Subject to Audit** check box, and select an **Audit Period** from the list.
6. Click **Create**. The records folder displays in the Exploring page. Click the Info icon for the new records folder. The Records Folder Information page displays “Subject to Audit: Yes” and displays the corresponding Audit Period.

Retention Schedule Interface Screens

The following screens are used to manage Retention Schedules:

- Series Interface Screens (page 8-38)
- Category Interface Screens (page 8-42)
- Folders Interface Screens (page 8-49)

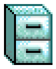
Series Interface Screens

The following screens are used to manage series:

- Create or Edit Series Page (page 8-39)
- Series Information Page (page 8-40)
- Select Retention Series, Folder or Category Screen (page 8-41)

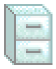
A series is indicated in the interface by a folder cabinet icon:

Figure 8-9 Series icon

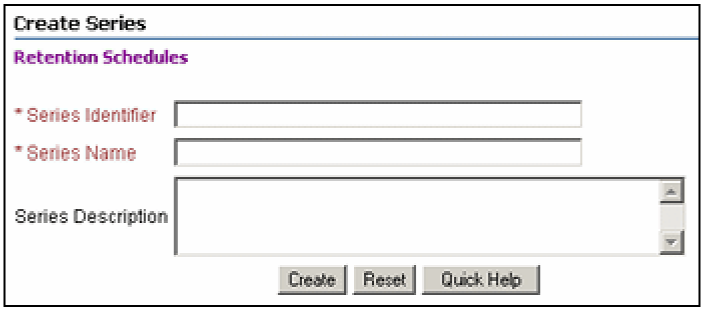


A hidden series icon appears as a more transparent image:

Figure 8-10 Hidden series icon



Create or Edit Series Page



Create Series

Retention Schedules

* Series Identifier

* Series Name

Series Description

Permissions: The Series.Create right is required to use these pages. This right is assigned by default to the ‘rmaadmin’ role.

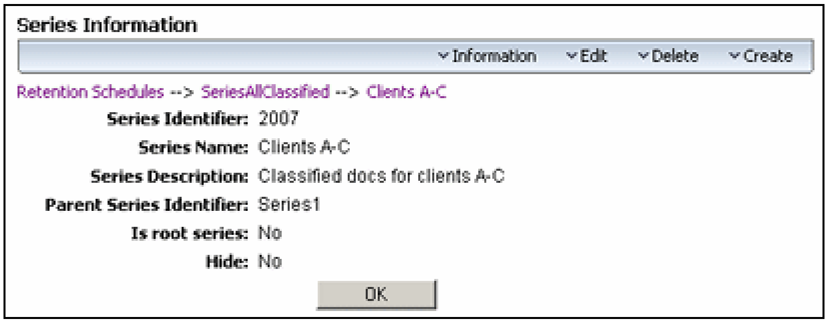
Use the Create page to create a new series. To access this page, open the **Browse Content** tray and click the **Retention Schedules** link. From the Page **Create** menu, click **Create Series**.

Use the Edit Series page to edit the name of an existing series. To access this page, open the **Browse Content** tray on the left, and click the **Retention Schedules** link. In the series row to view, select **Edit—Edit Series** from the Item **Actions** popup menu. You can also edit a series by selecting **Edit—Edit Series** from the Page menu on the Series Information Page (page 8-40).

Feature	Description
Series Identifier	Enter a unique identifier for the series. This field is view-only on the edit page. ❖ Required ❖ Maximum characters: 100
Series Name	Enter a name for the series. ❖ Required ❖ Maximum characters: 100
Series Description	Enter a description for the series. ❖ Optional ❖ Maximum characters: 1,000

Feature	Description
Create button (Create page only)	Creates the series.
Submit Update button (Edit page only)	Submits your updated edits.
Reset button	Resets the page to the initial default settings. If you are on an editing page, reset returns your original settings.

Series Information Page



Series Information

Retention Schedules --> SeriesAllClassified --> Clients A-C

Series Identifier: 2007
Series Name: Clients A-C
Series Description: Classified docs for clients A-C
Parent Series Identifier: Series1
Is root series: No
Hide: No

Anyone with the Series.Read right (assigned to all predefined DoD Edition roles) can view this page. To access the Series Information page, open the **Browse Content** tray, and click the **Retention Schedules** link. Choose **Information—Series Information** from the Item **Actions** popup menu. You can also click the item's Info icon (ⓘ).

The following information about a series is available:

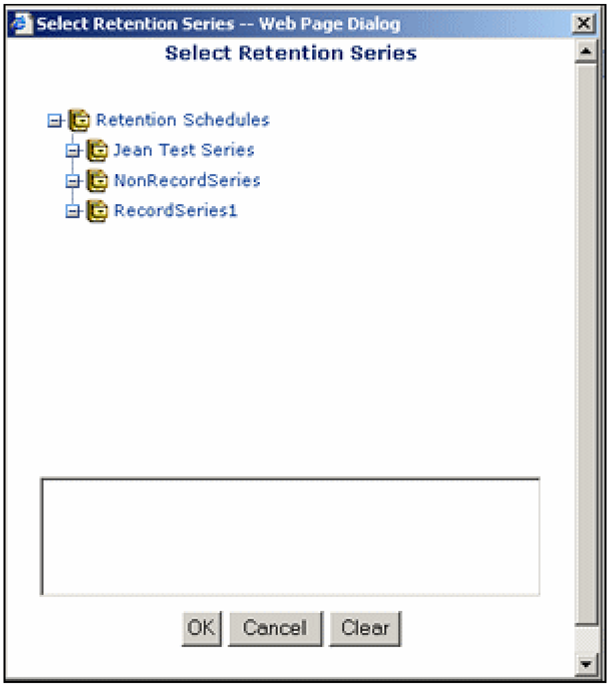
- **Series Identifier:** Displays the unique identifier for the series.
- **Series Name:** Displays the name of the series.
- **Series Description:** Displays the description of the series (only if a description was provided).
- **Parent Series Identifier:** If the series has a parent series, that is, it is a nested series, the Series Identifier is shown. If the series does not have a parent series, then this value displays a zero (0).
- **Is Root Series:** If this series is the main root node of the retention schedule, then this field displays "Yes." If this is not the main root of the retention schedule, then this

field displays "No." For more information about root nodes, see Configuring the Root Nodes (page 7-12).

- **Hide:** If the series is hidden, this field displays "Yes." If the series is not hidden, this field displays "No."

Depending on your assigned rights, you may also see the **Actions** Page menu. See Retention Schedule Menus (page 8-11) for details about the available options.

Select Retention Series, Folder or Category Screen



Use this screen to select a series, folder or category if you are moving it to another location. Series can be nested within a retention schedule.

Here are some tips for using this screen:

- To open the retention schedule, click the plus (+) sign or the icons to open it. Continue to click and expand the tree until you reach the location you want.
- The records and non-record content items you can select are indicated in red text.
- The breadcrumb trail for the location you select appears in the box.
- When you are finished selecting an object, click **OK**.

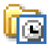
Category Interface Screens

The following screens are used to manage categories:

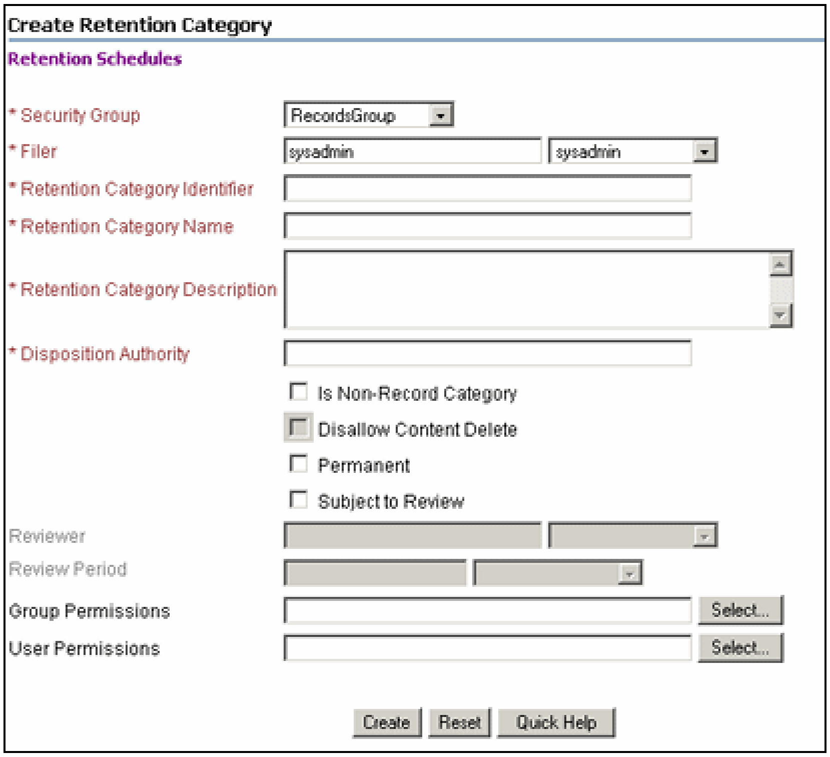
- Select Retention Series, Folder or Category Screen (page 8-41)
- Create or Edit Retention Category Page (page 8-42)
- Retention Category Information Page (page 8-48)
- Metadata History Page (page 8-48)
- Retention Category Information Page (page 8-48)

A category is indicated in the interface by a folder icon with a superimposed clock image:

Figure 8-11 Retention category icon



Create or Edit Retention Category Page



Create Retention Category

Retention Schedules

* Security Group	RecordsGroup
* Filer	sysadmin / sysadmin
* Retention Category Identifier	
* Retention Category Name	
* Retention Category Description	
* Disposition Authority	
	☐ Is Non-Record Category
	☐ Disallow Content Delete
	☐ Permanent
	☐ Subject to Review
Reviewer	
Review Period	
Group Permissions	Select...
User Permissions	Select...

Permissions: The Category.Create right is required to use the Create Retention Category page. This right is assigned by default to the 'rmaadmin' role.

Use the Create Retention Category page to create a new retention category for records or non-record content items. You can create retention category at the root node level, or within a series. To access the Create Retention Category page, open the **Browse Content** tray, and click the **Retention Schedules** link. Navigate to the location where you'll create a retention category. From the **Create** menu on the **Actions** list for the series or the Page menu, click **Create Retention Category**.

Use the Edit Retention Category page to edit an existing retention category. To access this page, open the **Browse Content** tray, and click the **Retention Schedules** link. Navigate to the retention category to edit. In the row for the retention category to edit, click **Edit—Edit Category** from the Item **Actions** popup menu. You can also edit a category by selecting **Edit—Edit Category** from the Page menu on the Retention Category Information Page (page 8-48)**.**

Permissions: The Category.Edit right is required to use the Edit Retention Category page. This right is assigned by default to the 'rmaadmin' role.

Feature	Description
Security Group	Displays the security group allowed access to the category. ❖ Default: RecordsGroup **Note:** This field is only displayed if default Content Server security is enabled in the Configure Records Management Page (page 7-2).
Account	Select an account allowed access to the category. ❖ Optional. **Note:** This field is only displayed if accounts are enabled in the content server. For more information, see the *Managing Security and User Access Guide.*

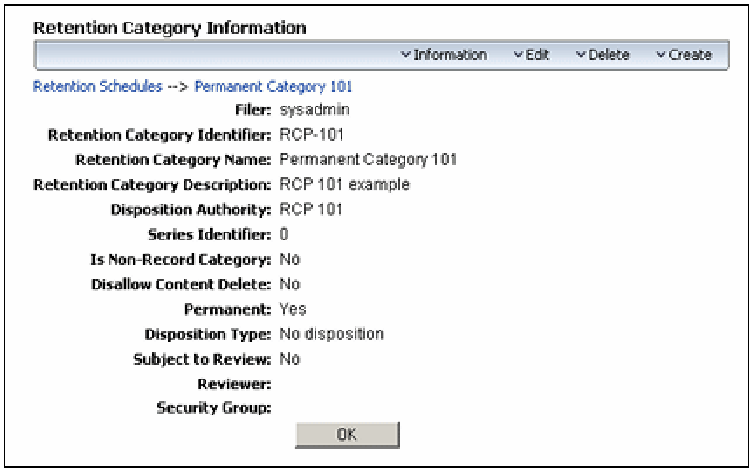
Feature	Description
Filer	Displays the name of the person who initially created the retention category. Select the filer from the options list. **Note:** This field is only displayed if default Content Server security is enabled in the Configure Records Management Page (page 7-2).
Retention Category Identifier	Enter a unique identifier for the retention category. ❖ Required. ❖ Maximum characters: 100. This field is view-only on the edit page.
Retention Category Name	Enter a name for the retention category. ❖ Required. ❖ Maximum characters: 100.
Retention Category Description	Enter a description of the retention category. ❖ Required. ❖ Maximum characters: 1,000.
Disposition Authority	Enter the code of the disposition authority for the retention category. The disposition authority code represents the legal authority who empowers a United States government agency to dispose of temporary records, or to transfer permanent records to the National Archives and Records Administration (NARA). The disposition authority for permanent records must be obtained from NARA. For certain temporary records, the authority must be obtained from the General Accounting Office (GAO). ❖ Required (for the government sector). Private sector organizations can indicate a person or department responsible for the records, or enter “none.” ❖ Maximum characters: 100.

Feature	Description
Is Non-Record Category check box	Indicates if the retention category contains non-record content items that have lifecycle schedules assigned to them. If you select this check box, the category is included in the Life Cycle dropdown list on the content check-in page. Non-record content is assigned the disposition instructions associated with the retention category selected in the dropdown list. If you clear this check box, you can only assign records to categories using the Browse button of the Category or Folders field on the record check-in page. ❖ Optional. ❖ Default: not selected (i.e., contains no non-record content). **Note:** For more information about checking in records, see the *Records Manager DoD Edition User Guide*.
Permanent check box	Indicates if a retention category contains permanent records. ❖ Optional. ❖ Default: not selected (i.e., contains no permanent records).

Feature	Description
Subject to Review check box (Create page only)	Indicates if a retention category contains items subject to review. All child record folders and records inherit the review status. For more information, see Attribute Inheritance (page 8-8). ❖ Optional. ❖ Default: not selected (i.e., not a record subject to review). After this check box is selected, the Reviewer and Review Period fields become available. To edit the review information for a retention category, you must access another page. For more information about managing categories, see the *Records Manager DoD Edition System Maintenance Guide*.
Disallow Content Delete	If checked, indicates the contents cannot be deleted.
Reviewer (Create page only)	Select the person responsible for reviewing records and non-record content items from the list. The user receives an e-mail notification when a review period for the category indicates a review cycle, as determined by the review period for the category. If a reviewer is not specified at the retention category level, the **Notify recipient** reviewer receives notifications for review. The system default reviewer is specified in the Configure Records Management Page (page 7-2). To edit the review information for a retention category, you must access another page.
Review Period text box and list (Create page only)	Enter an integer for the number of periods to cycle the content and select a corresponding period to go with the integer value from the Review Period list. To edit the review information for a retention category, you must access another page. For more information about managing reviews, see the *Records Manager DoD Edition System Maintenance Guide*.

Feature	Description
Group Permissions	Displays any group permissions assigned to the retention category. ❖ Optional. ❖ Maximum characters: 100. **Note:** This field is only displayed if ACL-based security is enabled. For more information, see Access Control Lists (ACLs) (page 5-16).
Select (Group) button	Opens the Select Alias screen so you can add groups to an access list and set permissions for each group. **Note:** This field is only displayed if ACL-based security is enabled. See Access Control Lists (ACLs) (page 5-16).
User Permissions	Displays any users granted access to the retention category. Click the Select button to define permissions at a user level. ❖ Optional. ❖ Maximum characters: 100. **Note:** This field is only displayed if ACL-based security is enabled. See Access Control Lists (ACLs) (page 5-16).
Select (Users) button	Opens the Select Users screen so you can add groups to an access list.and set permissions for each group. **Note:** This field is only displayed if ACL-based security is enabled. See Access Control Lists (ACLs) (page 5-16).
Create button (Create page only)	Creates the retention category and opens the Disposition Instructions Page (page 14-24).
Submit Update button (Edit page only)	Submits the edited retention category.
Reset button	Resets the page to the initial default settings.

Retention Category Information Page

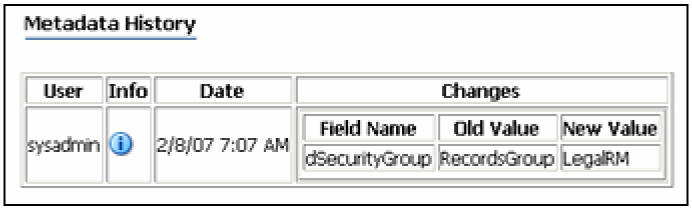

Retention Category Information
Information
Edit
Delete
Create
Retention Schedules --> Permanent Category 101
OK

Filer: sysadmin
Retention Category Identifier: RCP-101
Retention Category Name: Permanent Category 101
Retention Category Description: RCP 101 example
Disposition Authority: RCP 101
Series Identifier: 0
Is Non-Record Category: No
Disallow Content Delete: No
Permanent: Yes
Disposition Type: No disposition
Subject to Review: No
Reviewer:
Security Group:

Use this page to view information about a retention category. Anyone with the Category.Read right (assigned to all predefined DoD Edition roles) can view this page. To access the Retention Category Information page, open the **Browse Content** tray, and click the **Retention Schedules** link. Navigate to the retention category information to view. In the row for the retention category, click the Info icon (ⓘ). You can also click **Information—Retention Category Information** from the Item **Actions** popup menu.

The information displayed depends on the configuration of DoD Edition, and if optional fields were populated. See Retention Schedule Menus (page 8-11) for details about the available options on the Page menu.

Metadata History Page



User	Info	Date	Changes		
			Field Name	Old Value	New Value
sysadmin	ⓘ	2/8/07 7:07 AM	dSecurityGroup	RecordsGroup	LegalRM

Use this page to view the metadata history for a retention category—that is, a list of all changes that have been made to the editable category properties. To access the Metadata History page, open the **Browse Content** tray, and click the **Retention Schedules** link. Navigate to the appropriate retention category. Click **Information—Metadata History** from the Item Action popup menu. You can also **select Information—Metadata History** from the Page menu on the Retention Category Information Page (page 8-48).

Folders Interface Screens

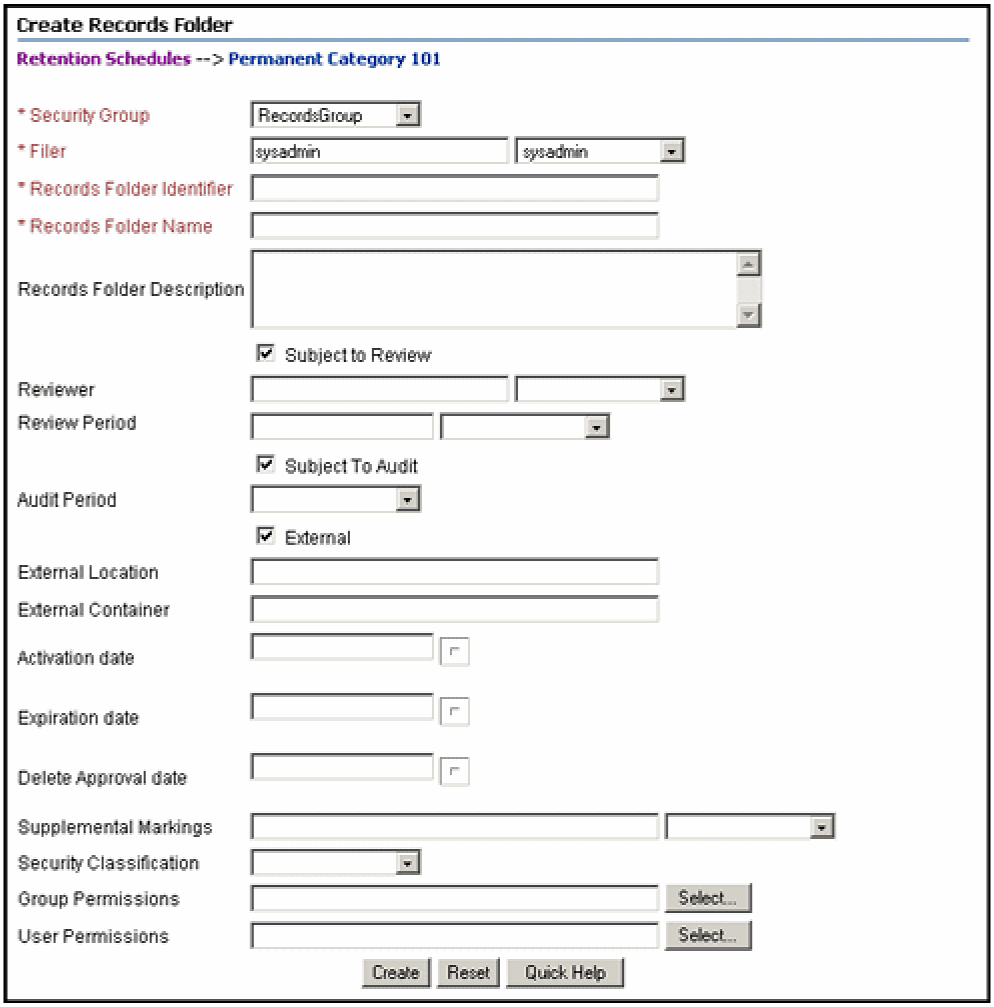
The following screens are used to manage folders:

- Create or Edit Records Folder Page (page 8-49)
- Records Folder Information Page (page 8-58)

A records folder is indicated in the Browse Content interface by the records folder icon:

Figure 8-12 Records folder icon

Create or Edit Records Folder Page



Create Records Folder

Retention Schedules --> Permanent Category 101

* Security Group	RecordsGroup ▾
* Filer	sysadmin · sysadmin ▾
* Records Folder Identifier	
* Records Folder Name	
Records Folder Description	
	☑ Subject to Review
Reviewer	▾
Review Period	▾
	☑ Subject To Audit
Audit Period	▾
	☑ External
External Location	
External Container	
Activation date	
Expiration date	
Delete Approval date	
Supplemental Markings	▾
Security Classification	▾
Group Permissions	Select...
User Permissions	Select...

Permissions: The Folder.Create right is required to use the Create Records Folder page. This right is assigned by default to the ‘rmaadmin’ role.

Use the Create Folder Category page to create a new records folder. To access this page, open the **Browse Content** tray, and click the **Retention Schedules** link. Navigate to the retention category or records folder location level where you’ll create the folder. Choose **Create—Create Records Folder** from the **Actions** list.

Permissions: The Folder.Edit right is required to use the Edit Records Folder page. This right is assigned by default to the ‘rmaadmin’ role.

Use the Edit Folder Category page to modify the properties of an existing records folder. To access this page, open the **Browse Content** tray and click the **Retention Schedules** link. Navigate to the retention category or records folder that contains the records folder to edit.Click **Edit—Edit Records Folder** from the Item **Actions** popup menu. You can also edit a folder by selecting **Edit—Edit Records Folder** from the Page menu on the Records Folder Information Page (page 8-58).

Feature	Description
Security Group	Displays the security group allowed access to the records folder. Set the security group permissions at the folder level if you do not want the records folder to inherit security settings from its parent category. ❖ Default: RecordsGroup. **Note:** This field is only displayed if Default Content Server security is enabled.
Account	Select an account allowed access to the records folder. ❖ Optional. **Note:** This field is only displayed if accounts are enabled in the content server. For more information, see the *Managing Security and User Access Guide*.

Feature	**Description**
Filer	Displays the filer who created the records folder. Select the filer from the options list. ❖ Required. ❖ Default: Privileged records user that is currently logged in. **Note:** This field is only displayed if default Content Server security is enabled in the Configure Records Management Page (page 7-2).
Records Folder Identifier	A unique identifier for the records folder. ❖ Required. ❖ Maximum characters: 100. This field is view-only on the edit page.
Records Folder Name	A name for the records folder. The name is not required to be unique. ❖ Required. ❖ Maximum characters: 100.
Records Folder Description	Describes the contents and purpose of the records folder. ❖ Optional. ❖ Maximum characters: 1,000.

Feature	Description
Freeze Reason	Available only if a freeze reason was entered when the records folder was frozen. Not applicable when creating a new records folder. If the records folder is frozen, the reason (if entered when freezing the folder) is populated in the Freeze Reason field. You can update the freeze reason from this location if you are editing a records folder on the Edit Records Folder page. The freeze reason is also displayed on the Records Folder Information Page (page 6-5). ❖ Recommended. ❖ Maximum characters: 100.
Subject to Review check box (Create page only)	Select the check box to enable the records folder as a record folder that is subject to review. If you want the folder to inherit the review information from a parent folder or category, clear the check box. Then enter a numeric value in the text box and select the associated period from the list. ❖ Optional. ❖ Default: not selected (i.e., not a record that is subject to review). **Note:** If a parent records folder or category has a review period of shorter duration than the review period set for the child folder, the child folder assumes the shorter review period. To edit the review information for a records folder, you must access another page.

Feature	Description
Reviewer (Create page only)	Select a reviewer for the records that are subject to review and are in this folder if you do not want to accept the system default reviewer specified in the Configure Records Management Page (page 7-2) or if you do not want to inherit the reviewer from the retention category or a parent records folder. The reviewer you select in this location will receive e-mail notification when it is time to review and cycle records. ❖ Optional. **Note:** Make sure that the reviewer you select has the Folder.EditReview right; otherwise, that person cannot mark a records folder as reviewed. To edit the review information for a records folder, you must access another page.
Review Period text box and list (Create page only)	Enter the number of review periods and select the review period from the list, which contains custom and predefined periods. Select the review period from the list. Required if the Subject to Review check box is selected. To edit the review information for a records folder, you must access another page.
Subject to Audit check box	Select this check box to indicate the records folder is subject to an audit. The Audit Period list becomes available. The "Audit Approval" indirect trigger must be properly set up. For more information, see Setting Up the "Audit Approval" Indirect Trigger (page 9-10). Clear the check box if the records folder is not subject to an audit.

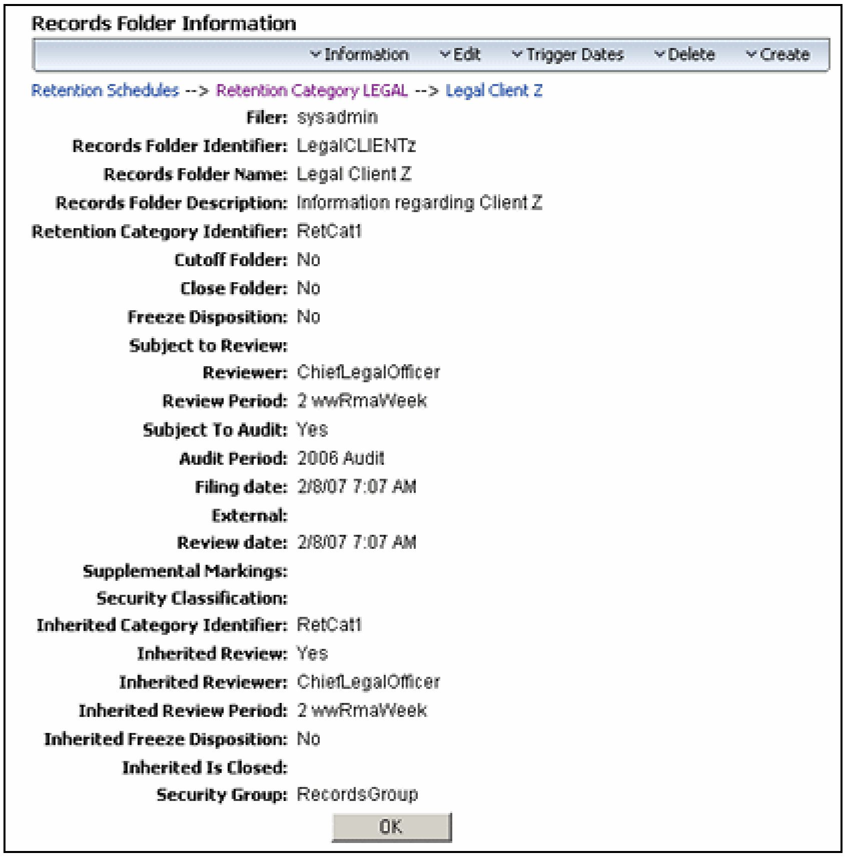
Feature	Description
Audit Period list	Select an audit period from the list, if the records folder is subject to audit. The Subject to Audit check box must be selected to enable the Audit Period list. The records administrator configures the audit periods. For more information, see the *Records Manager DoD Edition Installation Guid*e.
External check box	Select this check box to indicate that a records folder has a physical counterpart external to the Records Manager component. Selecting this check box enables the External Location and External Container check boxes.
External Location	Describes an external location for the records folder. This field is for records that have a physical counterpart. The External check box must be selected to use this field. ❖ Required if the External check box is enabled. ❖ Maximum characters: 100.
External Container	Enter a code or description for a physical container within which the records folder is filed. This field is for records that have a physical counterpart. The External check box must be selected to use this field. ❖ Optional. ❖ Maximum characters: 100.

Feature	Description
Activation Date	Enter a date or select it from the calendar component. The activation date corresponds to a date *within* a record but external to DoD Edition. For example, if a record corresponds to a legal contract, the activation date represents the actual date within the contract that the contract begins. The date format depends upon your user locale and preferences set in your system properties. You can also use this field to treat a records folder and its records as a single record from a disposition standpoint. ❖ Optional.
Expiration Date	Enter a date or select it from the calendar component. The expiration date is a deactivation date that corresponds to a record but is external to the DoD Edition component. For example, if a record corresponds to a legal contract, the expiration date represents the actual date the contract expires. ❖ Optional. **Note:** This record expiration date differs from the expiration date for documents in Content Server because the record can still be accessed in DoD Edition after deactivation. A document that has been expired in Content Server cannot be accessed after expiration.
Delete Approval date	Specify the date the delete action was approved for the records folder. After this date, the records folder can be deleted. ❖ Optional.

Feature	Description
Supplemental Markings	Contains any supplemental markings defined. Select one or more supplemental markings to secure the records folder. ❖ Optional. For more information, see Supplemental Markings Details (page 6-3).
Group Permissions	Displays any group permissions assigned to the records folder. Set group permissions at the folder level for the records folder to have its own security settings, rather than inheriting security settings from its parent retention category. ❖ Optional. ❖ Maximum characters: 100. **Note:** This field is only displayed if ACL-based security is enabled. For more information, see Access Control Lists (ACLs) (page 5-16).
Select (Group) button	Opens the Select Alias screen so you can add groups to an access list and set permissions for each group. **Note:** This field is only displayed if ACL-based security is enabled. For more information, see Access Control Lists (ACLs) (page 5-16).

Feature	Description
User Permissions	Displays users granted access to the records folder. Set permissions at the records folder level to set security at the records folder level, and if you do not want the records folder to inherit security settings from its parent retention category. ❖ Optional. ❖ Maximum characters: 100. **Note:** This field is only displayed if ACL-based security is enabled. For more information, see Access Control Lists (ACLs) (page 5-16).
Select (User) button	Opens the Select Users screen so you can add groups to an access list and set permissions for each group. **Note:** This field is only displayed if ACL-based security is enabled. For more information, see Access Control Lists (ACLs) (page 5-16).
Create button (Create page only)	Creates the records folder.
Submit Update button (Edit page only)	Submits your updated edits.
Reset button	Resets the page to the initial default settings. If you are on an editing page, reset returns your original settings.

Records Folder Information Page



Retention Schedules --> Retention Category LEGAL --> Legal Client Z

Filer: sysadmin
Records Folder Identifier: LegalCLIENTz
Records Folder Name: Legal Client Z
Records Folder Description: Information regarding Client Z
Retention Category Identifier: RetCat1
Cutoff Folder: No
Close Folder: No
Freeze Disposition: No
Subject to Review:
Reviewer: ChiefLegalOfficer
Review Period: 2 wwRmaWeek
Subject To Audit: Yes
Audit Period: 2006 Audit
Filing date: 2/8/07 7:07 AM
External:
Review date: 2/8/07 7:07 AM
Supplemental Markings:
Security Classification:
Inherited Category Identifier: RetCat1
Inherited Review: Yes
Inherited Reviewer: ChiefLegalOfficer
Inherited Review Period: 2 wwRmaWeek
Inherited Freeze Disposition: No
Inherited Is Closed:
Security Group: RecordsGroup

Permissions: The Folder.Read right is required to use this page. All predefined roles this right.

Use the Records Folder Information page to view information about a records folder. To access this page, open the **Browse Content** tray, and click the **Retention Schedules** link. Navigate to the appropriate records folder. In the row for the records folder, do one of the following:

- Click the Info icon (ⓘ).
- Click **Information—Records Folder Information** from the Item **Actions** popup menu.

The information displayed depends on the configuration for Records Manager DoD Edition, and if optional fields were populated.

Chapter

9

SETTING UP TRIGGERS

OVERVIEW

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 record or non-record content item state, completed processing of a preceding disposition action, retention period cutoff, and custom triggers, both regular and recurring.

This chapter covers the following topics:

Concepts

Tasks

Examples

- Global Triggers (page 9-13)
- Delayed Global Trigger (page 9-14)
- Dormant Global Trigger (page 9-14)
- Activating a Dormant Global Trigger (page 9-14)
- Custom Direct Trigger (page 9-14)

Interface

- Create or Edit Trigger Type Page (page 9-18)
- Trigger Information Page (page 9-22)
- Indirect Trigger Date Entries Page (page 9-23)

TRIGGER OVERVIEW

Two types of triggers are provided which can be used 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, you must have one of the following rights:

- **Admin.RecordManager**—This right allows you to view information about triggers.
- **Admin.Triggers**—In addition to viewing information about triggers, this right also allows you to create (add), edit, and delete triggers.

Tech Tip: 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 that trigger.

This section covers the following topics:

- System-Derived Triggering (page 9-3)
- Custom Triggers (page 9-4)

System-Derived Triggering

System-derived triggering uses the following built-in events or actions:

- Retention period cutoff
- Preceding (disposition) action
- Different record states

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 record or non-record 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 records or non-record content items are retained for three years after the end-of-year cutoff.

You can only specify retention periods for triggers for non-record content items if the `AllowRetentionPeriodWithCutoff` flag is enabled. This is enabled by default.

Negative Retention Periods

In previous versions of this product, a negative retention schedule could be supplied for a preceding action. This has now been changed so negative retention periods are available for non-record categories only if the following variables are enabled in the records_management_environments.cfg file:

- `AllowRetentionPeriodWithoutCutoff=1`. When this is 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 these are 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
```

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.

Content, Record, or Folder States

System-derived global triggers based on a record or folder state can be affected by an implicit or explicit change in an item or record or a records folder. An example of an implicit change is when a record has an activation date set in the future. The system is aware of the future activation date, and it activates the record at the indicated date. The change is implicit in that DoD Edition automatically changes the state of the record to active. The records administrator did not have to perform any explicit action other than indicating the future activation date of the record. An example of an explicit change in record state is when a records administrator manually cancels or expires a specific record. When a record assumes another trigger-dependent state, then the associated disposition rule operates on the record.

Custom Triggers

Custom triggers are defined explicitly by a records administrator. Custom triggers are more inclusive and less granular than a system-derived trigger based on record states. A custom trigger can affect all eligible records or non-record content items within a given retention category; whereas a system-derived trigger may only affect one record or non-record content item within a retention category, because it may be the only item that is in a given state.

Three types of custom triggers can be defined:

- Global triggers, which happen at a time defined by an administrator
- Custom direct triggers, whch use metadata fields as triggering events
- Custom indirect triggers, which occur on a regular schedule based on audit events

The triggers you create appear in the Triggering Events list of the Disposition Rules screen. For further information, see Chapter 14 (*Defining Disposition Instructions)*.

Access to creating, editing, and viewing information about triggers can be controlled by security settings. If access control list (ACL) security is enabled, you can restrict access to triggers by group and user permissions. If you use default Content Server security, then you can assign the trigger to a security group and designate the filer.

Global Triggers

Global triggers have an activation date. The activation date can be a past, present, or future date. You can create a trigger and delay the activation of a trigger for an indefinite amount of time until activation is required (that is, create a “dormant” trigger, which does not contain an activation date).

You 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 (that is, create a “dormant” trigger that does not contain an activation date).

Custom Direct Triggers

Use custom direct triggers 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 record or non-record content state, and on record, non-record content, or record folder date fields only. These triggers are not global triggers. They only affect a record or non-record content item that meets a given state. Unlike regular (global) or recurring event (indirect) triggers, you do not set an activation date explicitly for the custom direct trigger, or enable the custom direct trigger. Once created, the custom direct trigger is always active and ready to be used.

You can create a custom direct trigger with a date field, or a 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 record fields are used to activate the trigger for records, and the folder fields are used to activate the trigger for folders.

Indirect Triggers

Unlike a regular (global) trigger, an indirect trigger has a recurring life cycle. Audit Approval is the built-in indirect trigger. This trigger is based on a recurring audit event. It requires the Subject to Audit check box to be selected when checking in a record or non-record content item, and an audit period selected from the Audit list on the check-in page. For more information about checking in records and content, see the *Records Manager DoD Edition User Guide* and *Content Server User Guide*.

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. For instructions, see the *Records Manager DoD Edition Installation Guide*.

Managing Triggers

Several tasks are involved in managing triggers:

- Creating or Editing a Trigger (page 9-6)
- Viewing Trigger Information (page 9-8)
- Viewing Trigger References (page 9-9)
- Deleting a Trigger (page 9-9)
- Setting Up the “Audit Approval” Indirect Trigger (page 9-10)
- Defining Indirect Trigger Date Entries (page 9-11)
- Deleting an Indirect Trigger Date Entry (page 9-12)
- Disabling an Indirect Trigger Period (page 9-12)

Creating or Editing a Trigger

Use this procedure to create a new trigger. If you plan to assign more granular security settings on triggers then the default DoD Edition roles, then be sure you have enabled the access control list (ACL) security settings and assigned users to records roles and to an alias for any group permissions.

When creating an indirect trigger, make sure that the content field on which you are basing the custom indirect trigger has already been created in Content Server’s Configuration Manager utility, and that the period option list for the indirect trigger periods has been populated (see the *Records Manager DoD Edition Installation Guide* for details).

Permissions: The Admin.Triggers right is required to perform this action. This right is assigned by default to the ‘rmaprivileged’ and ‘rmaadmin’ roles.

1. Select **Configure—Triggers** from the Page menu on the Configure Records Management Page (page 7-2).

   The Configure Triggers Page (page 9-17) is displayed.

2. Select the type of trigger to create (Global, Custom Direct, or Indirect). Click **Add**.

The Create or Edit Trigger Type Page (page 9-18) is displayed.

3. (Optional) If the default Universal Content Management security is enabled, select a **Security Group** and **Author** from the lists. Otherwise, the default Security Group is always “RecordsGroup” and the author defaults to the user with the ‘rmaadmin’ or ‘rmaprivileged’ role who created the trigger, even if these fields are not displayed at the time the trigger was created.
4. (Optional) If your organization uses the accounts security model, indicate the **Account** for the trigger.
5. Enter a name up to 30 characters in the **Trigger Name** text box.
6. Enter specific Trigger Information:

   Global Triggers Only

   > Enter an **Activation Date**. If you do not enter an activation date, 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 you can change your database to accept more characters into this field.

   Custom Indirect Trigger

   > Select a **content field** on which the indirect trigger is based. The dropdown lists contains all available content fields. Select a **folders field** on which the indirect trigger is based. The dropdown lists contains all available folders fields.
7. (Optional) If ACL-based security is enabled, select **Group** and **User Permissions** for the trigger.
8. Click **Create**.

   A message is displayed saying that the trigger was created successfully.
9. Click **OK**.

Custom Indirect Triggers: You can now enter the recurring date periods for the trigger. For more information, see Defining Indirect Trigger Date Entries (page 9-11).

Use this procedure to modify the properties of an existing trigger. For example, you may need to change the activation date of a trigger, or change its security access.

Tech Tip: It is best practice not to use more than two fields at a time for a custom direct trigger, for processing and simplicity.

1. Select **Configure—Triggers** from the Page menu on the Configure Records Management Page (page 7-2).

   The Configure Triggers Page (page 9-17) is displayed.

2. Select the type of trigger to edit (Global, Custom Direct, or Indirect).

3. Click **Edit—Edit Trigger** from the Item **Actions** menu for the trigger to edit. You can also click the trigger name and select **Edit** from the Page menu on the Trigger Information Page (page 9-22) which is displayed.

   The Create or Edit Trigger Type Page (page 9-18) is displayed.

4. Make the desired changes to the applicable fields.

5. Click **Submit Update**.

   A message is displayed saying that the trigger was updated successfully.

6. Click **OK**.

Viewing Trigger Information

Permissions: Either the Admin.Triggers or Admin.RecordManager right is required to perform this action. The Admin.Triggers right is assigned by default to the ‘rmaprivileged’ and ‘rmaadmin’ roles, and the Admin.RecordManager right to the ‘rmaadmin’ role.

1. Select **Configure—Triggers** from the Page menu on the Configure Records Management Page (page 7-2).

   The Configure Triggers Page (page 9-17) is displayed.

2. Select the type of trigger to view (Global, Custom Direct, or Indirect).

3. Click the trigger name to view.

   The Trigger Information Page (page 9-22) is displayed.

4. When you finish viewing trigger information, click **OK**.

Viewing Trigger References

Use this procedure to view references to a trigger; that is, those disposition rules that use the trigger in their definitions.

Permissions: 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 'rmaprivileged' and 'rmaadmin' roles, and the Admin.RecordManager right to the 'rmaadmin' role.

1. Select **Configure—Triggers** on the Configure Records Management Page (page 7-2).

   The Configure Triggers Page (page 9-17) is displayed.

2. Select the type of trigger to view (Global, Custom Direct, or Indirect).
3. Click the trigger name to view.

   The Trigger Information Page (page 9-22) is displayed.

4. From the Page menu, click **References**.

   The Trigger References page is displayed. This page shows all category dispositions that the current trigger is referenced by, with a link to each of the referencing category disposition. If you click the link, the Disposition Information Page (page 14-28) of the referencing disposition is displayed.

5. When you finish viewing the reference information, click **OK**.

Deleting a Trigger

Use this procedure to delete a trigger. If a trigger is already in use, you must delete all references to a trigger before you can delete it. Triggers are referenced by triggering events in disposition rules. For more information, see Creating or Editing a Disposition Rule (page 14-13).

Permissions: The Admin.Triggers right is required to perform this action. This right is assigned by default to the 'rmaprivileged' and 'rmaadmin' roles. In addition, you must have delete permission (D) for the trigger's security group. **The 'rmaprivileged' role does not have this permission by default.**

1. Select **Configure—Triggers** on the Configure Records Management Page (page 7-2).

   The Configure Triggers Page (page 9-17) is displayed.

2. Select the type of trigger to view (Global, Custom Direct, or Indirect).

3. Navigate to the trigger to delete.
4. Click **Delete Trigger** on the trigger’s **Actions** menu.

   A message is displayed saying that the trigger was deleted successfully.
5. Click **OK**.

To delete multiple triggers, select the trigger checkboxes and click **Delete** on the Table menu.

Setting Up the “Audit Approval” Indirect Trigger

Use this procedure to specify the dates your organization requires for the Audit Approval recurring periods. The “Audit Approval” indirect trigger is the only built-in indirect trigger available at this time.

Permissions: The Admin.Triggers right is required to perform this action. This right is assigned by default to the ‘rmaprivileged’ and ‘rmaadmin’ roles.

1. Select **Configure—Triggers** on the Configure Records Management Page (page 7-2).

   The Configure Triggers Page (page 9-17) is displayed.
2. In the **Indirect Trigger Name** list, select **Audit Approval**, and click **Info**.

   The Trigger Information Page (page 9-22) is displayed. The **Built-in** label indicates “Yes.” The Content Field is mapped to “xAuditPeriod” and the Folders Field is mapped to “dAuditPeriod”.
3. Select **Indirect Trigger Date Information** on the Page menu.

   The Indirect Trigger Date Entries Page (page 9-23)) is displayed.
4. Click **Add**. The Create Indirect Trigger Date Entry page is displayed.
5. Select the **trigger period** which needs an activation date. You must have already populated the Trigger Period list in Content Server’s Configuration Manager utility.
6. The indirect trigger is **Enabled** by default. To disable the indirect trigger for performance reasons, or if you do not yet need the trigger enabled, clear the Enabled check box.
7. Enter an **activation date** for the trigger period. You can select the date from the Calendar icon. If you need to edit the time, you can do so directly in the Activation Date text box. Be sure to use the time format configured by your system defaults.

8. Click **Create**. The Trigger Date Entry information is added to the Indirect Trigger Date Entries for 'Audit Approval' page:
9. Repeat steps 5 through 8 to define dates for each indirect trigger period.

Defining Indirect Trigger Date Entries

Use this procedure to define the trigger date entries for each period for a custom or built-in indirect trigger. Make sure that the associated custom indirect trigger has been created and that the period option list for the indirect trigger periods has been populated (see the *Records Manager DoD Edition Installation Guide* for details).

Permissions: The Admin.Triggers is required to perform this action. This right is assigned by default to the 'rmaprivileged' and 'rmaadmin' roles.

To define a date entry (trigger period) for an indirect trigger, complete the following steps:

1. Select **Configure—Triggers** from the Configure Records Management Page (page 7-2).

   The Configure Triggers Page (page 9-17) is displayed.
2. Select the trigger from the **Indirect Trigger Name** list, and click **Info**.

   The Trigger Information Page (page 9-22) is displayed.
3. Click **Indirect Trigger Date Information** on the Page menu.

   The Indirect Trigger Date Entries Page (page 9-23) is displayed.
4. Click **Add**.

   The Create/Edit Indirect Trigger Date Entries Page (page 9-24) is displayed.
5. Define the indirect trigger date entries:
   a. Select a period from the **Trigger Period** list. You must manually populate this list using Content Server's Configuration Manager utility. For further information, see the online help or administration guides for Content Server.
   b. Select or clear the **Enabled** check box to enable or disable the indirect trigger.
   c. Enter an **Activation Date**.
   d. Click **Create**. The indirect trigger date entries populate on the Indirect Trigger Date Entries page, and the Trigger Period list is now populated with your defined period.

   Repeat this step to define dates for each period you need for the indirect trigger.

Deleting an Indirect Trigger Date Entry

Permissions: The Admin.Triggers right is required to perform this action. This right is assigned by default to the ‘rmaprivileged’ and ‘rmaadmin’ roles.

To delete a date entry (trigger period) for an indirect trigger, complete the following steps:

1. Select **Configure—Triggers** from the Configure Records Management Page (page 7-2).

   The Configure Triggers Page (page 9-17) is displayed.

2. Select **Delete** from the trigger’s Actions menu.

Disabling an Indirect Trigger Period

Use this procedure to disable, or “disarm,” an indirect trigger period at the date entry level. Disabling an indirect trigger period inactivates the trigger, but retains the trigger for archival purposes. You can disable the trigger period for both built-in and custom indirect triggers.

Permissions: The Admin.Triggers right is required to perform this action. This right is assigned by default to the ‘rmaprivileged’ and ‘rmaadmin’ roles.

1. Select **Configure—Triggers** from the Configure Records Management Page (page 7-2).

   The Configure Triggers Page (page 9-17) is displayed.

2. Select **Edit—Edit Trigger** from the trigger’s Actions menu.

   The Create or Edit Trigger Type Page (page 9-18) is displayed.

3. Select the trigger period to disable from the trigger period list, and click **Info**. The Create/Edit Indirect Trigger Date Entries Page (page 9-24) is displayed.

4. Clear the **Enabled** check box, and click **Submit Update**. The **Enabled** field for the Trigger Period you edited now displays “No.” Click the Configure Retention Schedule Components bread crumb link at the top of the page to return to the Configure Retention Schedule Components page.

TRIGGER EXAMPLES

This section provides several examples of the following different triggers:

- Global Triggers (page 9-13)
- Delayed Global Trigger (page 9-14)
- Dormant Global Trigger (page 9-14)
- Activating a Dormant Global Trigger (page 9-14)
- Custom Direct Trigger (page 9-14)

Permissions: The Admin.Triggers right is required to perform the tasks in these examples. This right is assigned by default to the ‘rmaprivileged’ and ‘rmaadmin’ roles.

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. Select Configure—Trigger from the Configure Records Management Page (page 7-2).

   The Configure Triggers Page (page 9-17) is displayed.

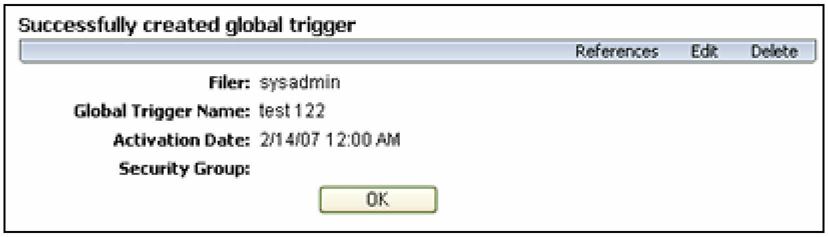
2. In the Global Triggers area, click **Add**. The Create or Edit Trigger Type Page (page 9-18) is displayed.

3. Enter a name up to 30 characters in the **Trigger Name** text box. For this example, type `Case 123 Closed`.

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 is displayed saying that the trigger was created successfully. The **Enabled** label indicates “Yes,” and the **Activation Date** is displayed.

Figure 9-13 Example: creating an active and enabled trigger



Successfully created global trigger

Filer: sysadmin

Global Trigger Name: test 122

Activation Date: 2/14/07 12:00 AM

Security Group:

Delayed Global Trigger

You can also create a global trigger with a future activation date. The activation of the trigger is delayed until the date and time that you specify. You can backdate trigger activation. To do so, use a future activation date when you create the global trigger.

Dormant Global Trigger

You can create a trigger with an activation date that is delayed until you enter an activation date. This is a dormant, inactive trigger. A dormant trigger is useful for event triggers when you know an event is going to occur, but you are not certain of the exact date it will occur. To avoid system processing overhead, do not enable the trigger. To view an example procedure on activating a trigger at a later date, see Activating a Dormant Global Trigger (page 9-14).

To create a dormant global trigger, do not enter an activation date when you create the trigger, but enter it at a later time.

Activating a Dormant Global Trigger

You can activate a disabled, dormant trigger that does not have an activation date set for the future. To do so, edit the trigger and enter the activation date.

Custom Direct Trigger

This example creates a custom direct trigger for a custom record field based on the termination date of an employee. Once the employee termination date is entered on the Content Info Update form, the direct triggers and the record begins its disposition processing. There are three parts to this example:

1. We create the custom record field for the Employee Termination Date using Content Server’s Configuration Manager utility.
2. In DoD Edition, we then create a custom direct trigger that keys off that date field.

3. As part of this example, we will also set up the disposition instruction that is activated by this custom trigger. The disposition instruction performs the cutoff when the employee termination date is entered, retains the record for 3 years, and then destroys the record. For more information about dispositions, see Chapter 14 (*Defining Disposition Instructions)*.
4. As a last step, we test the trigger to verify it is working correctly.

Creating the Record Field

To create the record field, complete the following steps:

1. Select **Admin Applets** from the **Administration** tray.

   The Administration Applets page for your server is displayed.
2. Click **Configuration Manager**.

   The Configuration Manager utility starts.
3. Click the **Information Fields** tabs, and click **Add**.

   The Add Custom Info Field screen is displayed.
4. Enter `EETermDate` in the **Field Name** box, and click **OK**.

   The Edit page for the field is displayed.
5. In the **Field Caption** box, enter “Employee Termination Date.”
6. In the **Field Type** list, select **Date**.
7. Make sure **Required** is not enabled; **User Interface** and **Search Index** are Enabled (typical defaults).
8. Click **OK**.
9. Click **Update Database Design**.
10. If using the Verity index engine, click **Rebuild Search Index**.

Creating the Custom Direct Trigger

Now we have a custom field so we can use it to build an example trigger.

1. Select **Configure—Triggers** from the Configure Records Management Page (page 7-2).

   The Configure Triggers Page (page 9-17) is displayed.
2. In the Custom Direct Trigger area, click **Add**.

The Create or Edit Trigger Type Page (page 9-18) is displayed.

3. Enter a name in the **Trigger Name** text box. For this example, type “EE Term Date.”
4. In the **Brief Description** box, enter “Employee Termination Date.”
5. In the **Content Date Field(s)** list, select **EETermDate**. The field is populated with “xEETermDate.”
6. Click **Create**.

   A message is displayed saying that the custom direct trigger was created successfully.

Setting Up the Disposition Instructions

This example creates disposition rules for a category named “Employees.” To create the category and disposition instruction, complete the following steps:

1. Open the **Browse Content** tray, and click the **Retention Schedules** link. The Exploring Series “Retention Schedule” page is displayed.
2. Click **Create—Create Retention Category** on the Page menu.

   The Create or Edit Retention Category Page (page 8-42) is displayed.
3. Enter `EE-RC-1` in the **Retention Category Identifier** box.
4. Enter `Employees` in the **Retention Category Name** box.
5. Enter a description in the **Retention Category Description** box. For this example, type `Employee Retention Category`.
6. (Required for U.S. Government Agencies) Enter the code of the authority for the disposition in the **Disposition Authority** box. For this example, type `EE-RC-1`.
7. Click **Create**. The Disposition Instructions Page (page 14-24) is displayed.
8. Create the first rule:
   a. Click **Add**. The Disposition Rule Screen (page 14-25) is displayed.
   b. In the **Triggering Event** list, look under ***Record State*** and select the new custom direct trigger called “EE Term Date.”
   c. In the **Disposition Action** list, select **Cutoff**.
   d. Click **OK**.
9. Create the second rule:
   a. Click **Add**. The Disposition Rule Screen (page 14-25) is displayed.
   b. In the **Triggering Event** list, select **Preceding Action**.

c. In the **Retention Period** fields, enter 3 and select **Calendar Years**.

d. In the **Disposition Action** list, select **Destroy**.

e. Click **OK**.

f. Click **Submit Update**. The successfully updated disposition message is displayed with a summary of the disposition:

10. Click **OK**.

Verifying the Custom Direct Trigger

To test the trigger enter an expiration date for a test employee record or non-record content item in the Info Update Form, which you access from the Update option in the Actions list of the content information page. The record or non-record content item begins disposition processing on the cutoff date. If you check the life cycle for the record or non-record content item, you can see the dates are already set for the processing.

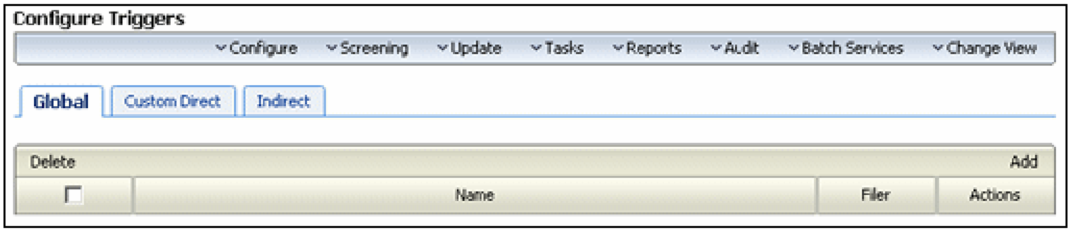
TRIGGERS INTERFACE

Similar pages are used to create Global Triggers, Custom Direct Triggers and Indirect Triggers. This section uses the Custom Direct Trigger interface pages as an example of these interface screens. In the field descriptons an indication is given to where the field is used for specific trigger types.

The following screens are used to manage triggers:

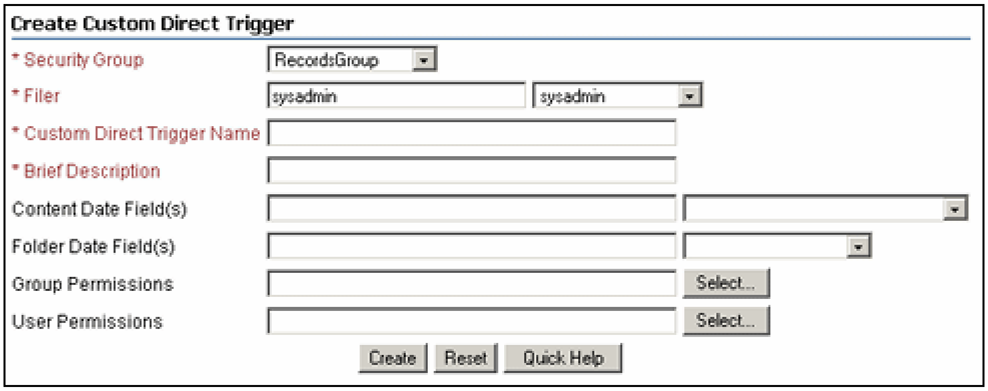
- Create or Edit Trigger Type Page (page 9-18)
- Trigger Information Page (page 9-22)
- Indirect Trigger Date Entries Page (page 9-23)
- Create/Edit Indirect Trigger Date Entries Page (page 9-24)

Configure Triggers Page



This page is used to select a type of trigger or a trigger for use. To access this page, click **Configure—Triggers** from the Configure Records Management Page (page 7-2).

Create or Edit *Trigger Type* Page



Create Custom Direct Trigger

* Security Group: RecordsGroup

* Filer: sysadmin | sysadmin

* Custom Direct Trigger Name:

* Brief Description:

Content Date Field(s):

Folder Date Field(s):

Group Permissions:

User Permissions:

Use the Create *Trigger Type* page to define a new trigger. To access this page, select a trigger type and click **Add** from the Configure Triggers Page (page 9-17).

Use the Edit *Trigger Type* page to modify the properties of an existing trigger. To access this page, select a trigger type and select **Edit—Edit Trigger** from a trigger's Item **Actions** popup menu. You can also click the trigger name and select **Edit** from the Trigger Information Page (page 9-22).

When you select a date from the list, the Content Date metadata fields are automatically prefixed with an 'x', and the Folder Date metadata fields are prefixed with a 'd'.

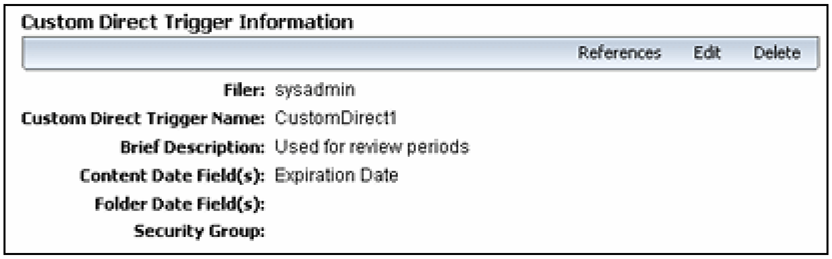
Feature	Description
Security Group	Displays the security group allowed access to the trigger. ❖ Default: RecordsGroup **Note:** This field is only displayed if Default Content Server security is enabled on the Configure Records Management Page (page 7-2).

Feature	Description
Account	Select an account that is allowed access to the trigger. ❖ Optional. **Note:** This field is only displayed if accounts are enabled in the Content Server. For more information, see the administrator documentation for Content Server.
Filer/Author	Displays the author of the trigger. Select the author the options list if you are not the author. ❖ Required. ❖ Default: Privileged records user that is currently logged in. **Note:** This field is only displayed if Default Content Server security is enabled on the Configure Records Management Page (page 7-2).
Trigger Name	Enter a name for the trigger. The name of the trigger appears in the ***Custom Triggers*** section of the **Triggering Event** options list in the Disposition Rule Screen (page 14-25). If this is an indirect trigger, the name appears in the **Recurring Custom Triggers** section. ❖ Required. ❖ Maximum characters: 100. This field is view-only on the edit page.
Brief Description *(Custom direct triggers only)*	Enter a brief description of the trigger. ❖ Required. ❖ Maximum characters: 100.

Feature	**Description**
Content Date Field(s) *(Custom direct triggers only)*	Select one or more date-related content fields from the list. ❖ Optional. ❖ Maximum characters: 100. **Note:** The New Revision Date option in the list is available only if the Enable New Revision Date Trigger Field option was selected during installation. 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 then stamped with the date of the new revision. This enables you to create retention rules such as “Delete if not updated in *x* number of years.”
Folder Date Field(s) *(Custom direct triggers only)*	Select one or more record folder date fields from the list. All available record folder date fields are available, including any custom record folder date fields. ❖ Optional. ❖ Maximum characters: 100.
Enabled check box *(Global triggers only)*	Activates or disarms the trigger. To disable the trigger, clear the check box. ❖ Optional. ❖ Default: Enabled is selected and the trigger is active according to the set activation date.
Activation Date *(Global triggers only)*	Specify the date when a trigger is activated. If you do not enter an activation date, an enabled trigger is delayed indefinitely (it is a dormant trigger). You can enter an activation at a later time. To view an example, see Dormant Global Trigger (page 9-14). ❖ Optional.

Feature	Description
Group Permissions	Displays any group permissions assigned to the trigger. ❖ Optional. ❖ Maximum characters: 100. **Note:** This field is only displayed if ACL-based security is enabled on Configure Records Management Page (page 7-2)
Select (Group) button	Opens the Select Alias screen so you can add groups to an access list and set permissions for each group. **Note:** This field is only displayed if ACL-based security is enabled on the Configure Records Management Page (page 7-2).
User Permissions	Displays users granted access to the trigger. ❖ Optional. ❖ Maximum characters: 100. **Note:** This field is only displayed if ACL-based security is enabled on the Configure Records Management Page (page 7-2).
Select (Users) button	Opens the Select Users screen so you can add groups to an access list and set permissions for each group. **Note:** This field is only displayed if ACL-based security is enabled on the Configure Records Management Page (page 7-2).
Create button (Create page only)	Creates the trigger.
Submit Update button (Edit page only)	Submits the edited trigger.
Reset button	If you are creating a new trigger, this resets the page to its initial default settings. If you are editing an existing trigger, this returns your original settings.

Trigger Information Page



Custom Direct Trigger Information

Filer: sysadmin
Custom Direct Trigger Name: CustomDirect1
Brief Description: Used for review periods
Content Date Field(s): Expiration Date
Folder Date Field(s):
Security Group:

Similar pages are used to view information about Global Triggers, Custom Direct Triggers and Indirect Triggers. This section uses the Custom Direct Trigger interface pages as an example of these interface screens. In the field descriptons an indication is given as to where the field is used for specific trigger types.

Permissions: Either the Admin.Triggers or Admin.RecordManager right is required to use this page. The Admin.Triggers right is assigned by default to the 'rmaprivileged' and 'rmaadmin' roles, and the Admin.RecordManager right to the 'rmaadmin' role.

To access a Trigger information page, select **Configure—Triggers** from the Configure Records Management Page (page 7-2). On the Configure Triggers Page (page 9-17) navigate to the type of trigger and click the trigger to view.

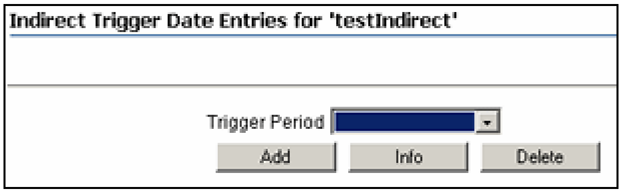
Depending on the type of trigger viewed, different information will appear.

If you have the Admin.Triggers right, the page includes a menu which provides the following options:

- **Indirect Trigger Date Information *(Indirect Trigger Information Page Only)***: Used to set recurring dates and periods for the indirect trigger. See Defining Indirect Trigger Date Entries (page 9-11).
- **Edit**: Used to edit the current indirect trigger. See Creating or Editing a Trigger (page 9-6).
- **Delete**: Used to delete the current indirect. See Deleting a Trigger (page 9-9).
- **References**: Enables you to see trigger references.

Note: You cannot edit or delete the built-in Audit Approval indirect trigger.

Indirect Trigger Date Entries Page



Indirect Trigger Date Entries for 'testIndirect'

Permissions: The Admin.Triggers right is required to work with indirect trigger date entries. This right is assigned by default to the ‘rmaprivileged’ and ‘rmaadmin’ roles.

Use the Indirect Trigger Date Entries page to create, view information about, edit, and delete date entries for indirect triggers. To access the page, select **Configure—Triggers** from the Configure Records Management Page (page 7-2). Select the trigger from the **Indirect Trigger Name** list, and click **Info**. Select **Indirect Trigger Date Information** from the Page menu.

Feature	**Description**
Trigger Period	Displays the name of the trigger period.
Enabled	Specifies if the trigger date entry is enabled.
Trigger Period option list	Contains a list of Trigger Periods from which you can add, find information for, or delete.
Add button	Opens the Create/Edit Indirect Trigger Date Entries Page (page 9-24) so that you can define the periods.
Info button	Opens the Information page for the selected Trigger Period.
Delete button	Deletes the date entry period selected in the Trigger Periods list.

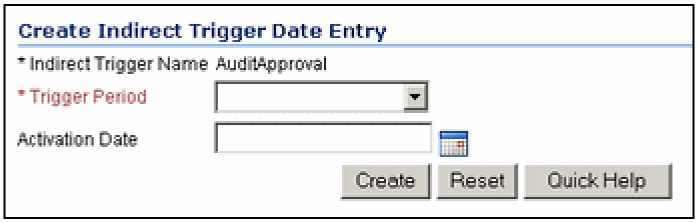
Note the following considerations:

- Click **Add** to define an indirect trigger date entry.

  The Create/Edit Indirect Trigger Date Entries Page (page 9-24) is displayed.

- If there are already trigger date entries defined, select one from the **Trigger Period** list, and click **Info** to view the date information.

Create/Edit Indirect Trigger Date Entries Page



Create Indirect Trigger Date Entry

* Indirect Trigger Name AuditApproval

* Trigger Period

Activation Date

Permissions: The Admin.Triggers right is required to use this page. This right is assigned by default to the ‘rmaprivileged’ and ‘rmaadmin’ roles.

Use the Create page to define the trigger period, enable or disable the trigger, and set an activation date for an indirect trigger. To access this page, select **Configure—Triggers** from the Configure Records Management Page (page 7-2). In the Indirect Trigger area, click **Add**.

Use the Edit page to modify the properties of an existing indirect trigger date entry. **Configure—Triggers** from the Configure Records Management Page (page 7-2). In the Indirect Trigger area, click **Edit** from a trigger’s Item Action popup menu or click on the trigger name and select **Edit** from the Trigger Information Page (page 9-22).

Feature	**Description**
Indirect Trigger Name	Displays the name of the indirect trigger for which you are setting the dates. This field is view-only on both the create and the edit pages.
Trigger Period	Displays the name of the indirect trigger period for which you are setting the dates. This field is view-only on the edit page.
Activation Date	Enter an activation date for the indirect trigger.
Create button (Create page only)	Creates the indirect trigger.
Submit Update button (Edit page only)	Submits the edited trigger.

Feature	Description
Reset button	If you are creating a new trigger, this resets the page to its default settings. If you are editing an existing trigger, this returns your original settings.

Chapter

10

Configuring Time Periods

Overview

Periods define a length of time. They are associated with retention periods for dispositions and with review periods for cycling content that is subject to review.

This chapter covers the following topics:

Concepts

Tasks

Example

Interface

USING TIME PERIODS

Three types of time periods are used in retention:

- **Custom**—A custom period has a defined start date and time that does not typically correspond 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.

You cannot edit or delete built-in periods. You can edit any periods you create, and you can delete any periods you create if the periods are not in use.

To work with periods, you must have one of the following rights:

- **Admin.Triggers**—This right allows you to view information about periods.
- **Admin.RecordManager**—In addition to viewing information about periods, this right also allows you 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 available for your use.

This section covers the following topics:

MANAGING TIME PERIODS

The following tasks are used when managing time periods:

- Creating or Editing a Custom Time Period (page 10-3)
- Viewing Period Information (page 10-4)
- Viewing Period References (page 10-4)
- Deleting a Custom Period (page 10-5)

Creating or Editing a Custom Time Period

Use this procedure to create a period 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.

Permissions: The Admin.RecordManager right is required to perform this action. This right is assigned by default to the ‘rmaadmin’ role.

1. Select **Configure—Periods** from the Configure Records Management Page (page 7-2).

   The Configure Periods Page (page 10-7) is displayed.
2. In the Period Name area, click **Add**.

   The Create or Edit Period Page (page 10-7) is displayed.
3. Enter a name for the period in the **Period Name** text box.
4. Select the type of time period: **Calendar, Fiscal,** or **Custom** in the **Period Type** list.
5. Click the calendar icon and select a custom start time. The date and default time display in the **Custom Start Time** box. If you do not want to accept the default time, edit the time within the text box.
6. Enter an integer value in the **Length** text box, and select the corresponding unit from the **Length** list.
7. Enter a label to describe the end of the period in the **Label for end of period** text box.
8. Click **Create**.

   A message is displayed saying that the period was created successfully, with the period information.
9. Click **OK**.

Permissions: The Admin.RecordManager right is required to perform this action. This right is assigned by default to the ‘rmaadmin’ role.

To edit a time period, complete the following steps:

1. Select **Configure—Periods** from the Configure Records Management Page (page 7-2).

   The Configure Periods Page (page 10-7) is displayed.

2. Select **Edit Period** from the Item Action popup menu for the period to edit. You can also click a period name and select Edit from the Period Information Page (page 10-10).

   The Create or Edit Period Page (page 10-7) is displayed.

3. Edit the appropriate information.

4. Click **Submit Update**.

   A message is displayed saying that the period was updated successfully.

5. Click **OK**.

Viewing Period Information

Permissions: Either the Admin.Triggers or Admin.RecordManager right is required to perform this action. The Admin.Triggers right is assigned by default to the ‘rmaprivileged’ and ‘rmaadmin’ roles, and the Admin.RecordManager right to the ‘rmaadmin’ role.

1. Select **Configure—Periods** from the Configure Records Management Page (page 7-2).

   The Configure Periods Page (page 10-7) is displayed.

2. Click the period to view from the **Period Name** list.

   The Period Information Page (page 10-10) is displayed.

3. When you finish viewing the information, click **OK**.

Viewing Period References

Use this procedure to view references to a period; that is, those categories, folders, and disposition rules that use the period in their definitions. Generally, you will want to view period references to determine why you can’t delete a custom period.

Permissions: Either the Admin.Triggers or Admin.RecordManager right is required to perform this action. The Admin.Triggers right is assigned by default to the ‘rmaprivileged’ and ‘rmaadmin’ roles, and the Admin.RecordManager right to the ‘rmaadmin’ role.

To view period references, complete the following steps:

1. Select **Configure—Periods** from the Configure Records Management Page (page 7-2).

The Configure Periods Page (page 10-7) is displayed.

2. Click the period to view from the **Period Name** list.

   The Period Information Page (page 10-10) is displayed.

3. From the Page menu, click **References**. The Period References page is displayed. This page shows all folders, categories, and/or category dispositions that the current period is referenced by, with a link to each of the referencing items. If you click any of the links, the associated information page for that item is displayed.

4. When you finish viewing the reference information, click **OK**.

Deleting a Custom Period

You cannot delete built-in periods. Before you can delete a period, you must make sure that the period is not referenced by a retention period within a disposition rule for a category, or by a review period for a record, records folder, or retention category.

Permissions: The Admin.RecordManager right is required to perform this action. This right is assigned by default to the 'rmaadmin' role.

1. Select **Configure—Periods** from the Configure Records Management Page (page 7-2).

   The Configure Periods Page (page 10-7) is displayed.

2. Select **Delete Period** from a period's Item Action popup menu. You can also click the period to view from the **Period Name** list and select Delete on the Period Information Page (page 10-10).

   A message is displayed saying that the period was deleted successfully.

3. Click **OK**.

Example: Creating a Custom Period

This example demonstrates creating a custom period with the following characteristics:

- The custom period name is "School Year 2005-2006."
- The custom start time is September 5th, 2005, 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 2005.”

Permissions: The Admin.RecordManager right is required to perform the tasks in this example. This right is assigned by default to the ‘rmaadmin’ role.

To create a custom school period, complete the following steps:

1. Select **Configure—Periods** from the Configure Records Management Page (page 7-2).

   The Configure Periods Page (page 10-7) is displayed.

2. In the Period Name area, click **Add**. The Create or Edit Period Page (page 10-7) is displayed.

3. In the **Period Name** box, enter `School Year 2005-2006`.

4. By default, the **Custom** option is already selected in the **Period Type** list. Leave the Custom option selected.

5. Click the calendar icon and select a custom start date: September 5, 2005. The date and default time display 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 a “`9`.” Make sure you specify the date according to the format used by your system locale.

6. In the **Length** box, enter the length of the custom period in the text box, which is `9` and select the **Months** option from the list.

7. In the **Label for end of period** box, enter `End of School Year 2005-2006`.

8. Click **Create**.

   A message is displayed saying that the period was created successfully.

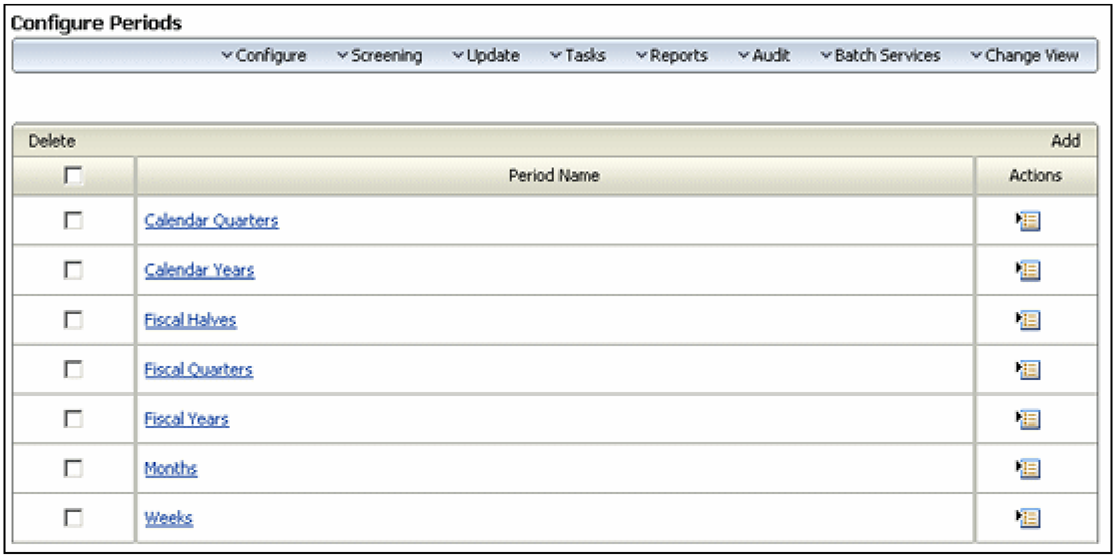
9. Click **OK**.

Time Period Interface

The following screens are used when managing time periods:

- Configure Periods Page (page 10-7)
- Create or Edit Period Page (page 10-7)
- Period Information Page (page 10-10)

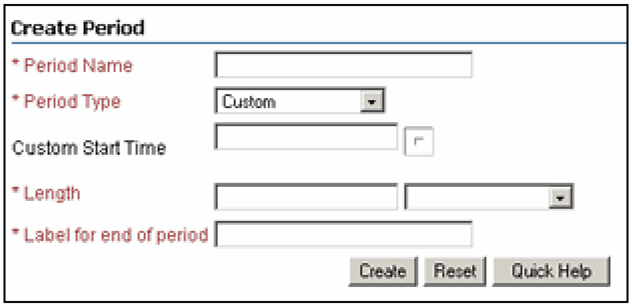
Configure Periods Page



□	Period Name	Actions
□	Calendar Quarters	
□	Calendar Years	
□	Fiscal Halves	
□	Fiscal Quarters	
□	Fiscal Years	
□	Months	
□	Weeks	

This page is used to select a period for editing or to add a new period. To access this page, select Configure—Periods from the Configure Records Management Page (page 7-2). The menu at the top of this page is the same menu as that on the Configure Records Management Page (page 7-2). See Configuration Page Menus (page 7-9) for details.

Create or Edit Period Page



* Period Name	
* Period Type	Custom
Custom Start Time	
* Length	
* Label for end of period	

Permissions: The Admin.RecordManager right is required to use this screen. This right is assigned by default to the ‘rmaadmin’ role.

Use the Create page to define a new period. To access this page, select **Add** from the Configure Periods Page (page 10-7).

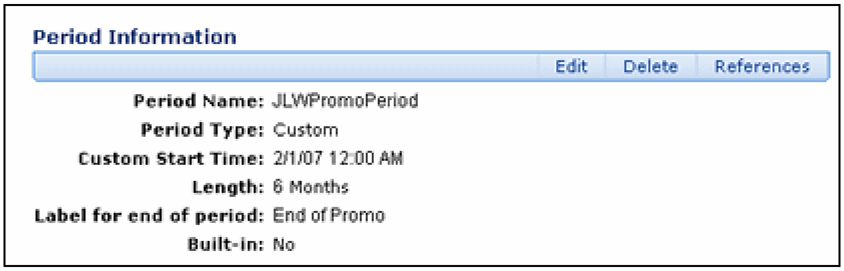
Use the Edit page to modify the properties of an existing period. To access this page, select **Edit Period** from a the Item Action popup menu for a listed period on the Configure Periods Page (page 10-7). You can also click on a Period name and select **Edit** from the Period Information Page (page 10-10).

Feature	**Description**
Period Name	Enter a name for the period. The name appears in the Period options lists, such as the review period lists or retention period lists. ❖ Maximum characters: 30. ❖ Required. This field is view-only on the edit page.
Period Type	Required. Select the type of period: ❖ **Fiscal**—A period based on the fiscal year as defined by your organization. The start date of the fiscal year is set in the Configure Records Management Page (page 7-2). Some fiscal periods are already created (built-in equals “Yes”). Any fiscal period you create is a “custom” fiscal period (the Built-in label on the Period information page indicates “No.”) ❖ **Calendar**—A period based on the Gregorian calendar year (i.e., starting with January 1). Some calendar periods are already created (built-in equals “Yes”). Any calendar period you create is a “custom” calendar period (the Built-in label on the Period information page indicates “No.”) ❖ **Custom (default)**—A period based on any fiscal or calendar year foundation. 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.” Some custom periods are already created (built-in equals “Yes”). Any custom period you create is a “custom” custom period (Built-in is “No.”).

Feature	Description
Custom Start Time	Displays the start date and time for a custom period. The selected Period Type must be “Custom” to enable the Custom Start Time field. Click the calendar icon to choose a date. The date and time appear in the format according to your User Locale and Content Server system properties. For more information, see administration documentation for Content Server. Required if the Custom Period Type is selected. Default time: 12:00 AM (midnight). You can edit the date and time within the text box.
Length box	An integer value for the length of the period. Required.
Length list	The period length. Available options are: ❖ Years ❖ Months ❖ Weeks ❖ Days Default: Blank. Required.
Label for end of period	A display label for the end of the period. The label you enter for the end of a custom period appears in the Triggering Event (“After”) fields in dispositions. ❖ Maximum characters: 30. ❖ Required.
Create button (Create page only)	Creates the defined period.
Submit Update button (Edit page only)	Submits your updated edits.

Feature	Description
Reset button	If you are creating a new period, this resets the page to its initial default settings. If you are editing an existing period, this resets your original settings.

Period Information Page



Period Information

Period Name: JLWPromoPeriod
Period Type: Custom
Custom Start Time: 2/1/07 12:00 AM
Length: 6 Months
Label for end of period: End of Promo
Built-in: No

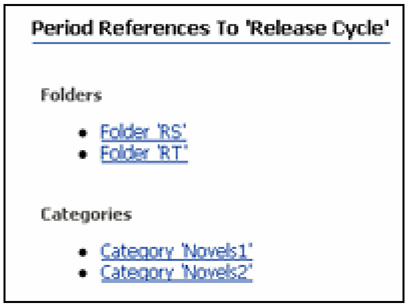
Permissions: Either the Admin.Triggers or Admin.RecordManager right is required to use this page. The Admin.Triggers right is assigned by default to the ‘rmaprivileged’ and ‘rmaadmin’ roles, and the Admin.RecordManager right to the ‘rmaadmin’ role. With the Admin.Triggers right, you can only view information about periods. With the Admin.RecordManager right, you can also add, edit, and delete periods.

Use this page to view information about a period. To access this page, click a period name on the Configure Periods Page (page 10-7).

You can also use this page to edit a period, delete a period, or view references to a period.

The Built-in label indicates if a period was a predefined, out-of-the box period. A period that an administrator creates 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 you cannot edit a predefined period. The Actions list is not available to any users other than those with the Admin.RecordManager right.

Period Reference Page



Period References To 'Release Cycle'

Folders

- Folder 'RS'
- Folder 'RT'

Categories

- Category 'Novels1'
- Category 'Novels2'

This page is used to view those objects which reference a particular period. To access this page, click **Reference** on the Period Information Page (page 10-10).

Chapter

11

CUSTOM METADATA FIELDS

OVERVIEW

If your organization has unique needs for metadata fields for retention categories or records folders, you can easily customize the application to include the fields. Depending on the field characteristics, the new custom fields are displayed in the Create Retention Category or Create Records Folder pages, in addition to the edit and information pages for those retention schedule objects. See Chapter 8 *(Setting Up a Retention Schedule)* for details.

Custom metadata fields are added to the bottom of the Create Retention Category or Create Records Folder pages. The order in which the custom metadata fields appear depends on the order you indicate in the custom metadata fields box. You can easily arrange the fields using the arrows near the custom metadata box.

This chapter covers the following topics:

Tasks

Examples

Interface

- Create/Edit Metadata Field Page (page 11-8)
- Metadata Information Page (page 11-11)

MANAGING CUSTOM METADATA

The following tasks are used when managing custom metadata:

- Creating or Editing Custom Metadata Fields
- Deleting a Custom Metadata Field

Important: If you plan to use an option list with the custom field, the option list must be created and populated prior to creating the custom field. See the *Managing Repository Content Guide* for details on creating option lists.

Creating or Editing Custom Metadata Fields

The following information is a general navigational procedure. To view a specific example, see Creating a Custom Category Metadata Field (page 11-4) or Creating a Custom Folder Metadata Field (page 11-5).

Permissions: The Admin.RecordManager right is required to perform this action. This right is assigned by default to the ‘rmaadmin’ role.

1. Select **Configure—Metadata Sets—Retention Categories** or **Configure—Metadata Sets—Records Folders** from the Configure Records Management Page (page 7-2).

   The Fields for Metadata Page (page 11-6) is displayed.

2. Click **Create Field**.

   The Create/Edit Metadata Field Page (page 11-8) is displayed.

3. Complete the metadata fields, and click **OK**.
4. Click **Submit Update**.

Use this procedure to edit a custom retention category or records folder metadata field.

Permissions: The Admin.RecordManager right is required to perform this action. This right is assigned by default to the ‘rmaadmin’ role.

1. Select **Configure—Metadata Sets—Retention Categories** or **Configure—Metadata Sets—Records Folders** from the Configure Records Management Page (page 7-2).

   The Fields for Metadata Page (page 11-6) is displayed.

2. Select **Update Field** from a field's **Actions** popup menu. You can also click the field's Info icon or name and select **Update Field** from the Metadata Information Page (page 11-11).

   The Create/Edit Metadata Field Page (page 11-8) is displayed. Make your changes, and click **OK**. Repeat for each field to edit.

3. Click **Submit Update**.

Deleting a Custom Metadata Field

Permissions: The Admin.RecordManager right is required to perform this action. This right is assigned by default to the 'rmaadmin' role.

To delete a custom category or folder metadata field, complete the following steps:

1. Select **Configure—Metadata Sets—Retention Categories** or **Configure—Metadata Sets—Records Folders** from the Configure Records Management Page (page 7-2).

   The Fields for Metadata Page (page 11-6) is displayed.

2. Select **Delete Field** from a field's Item **Actions** popup menu. You can also click the field's Info icon or name and select **Delete Field** from the Metadata Information Page (page 11-11).

3. You are prompted to confirm the deletion. Select **Yes** to delete the field. Choose **No** to retain the field.

EXAMPLES

The following examples are provided:

- Creating a Custom Category Metadata Field (page 11-4)
- Creating a Custom Folder Metadata Field (page 11-5)

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 an SKU (Stock Keeping Unit).

Permissions: The Admin.RecordManager right is required to perform this action. This right is assigned by default to the ‘rmaadmin’ role.

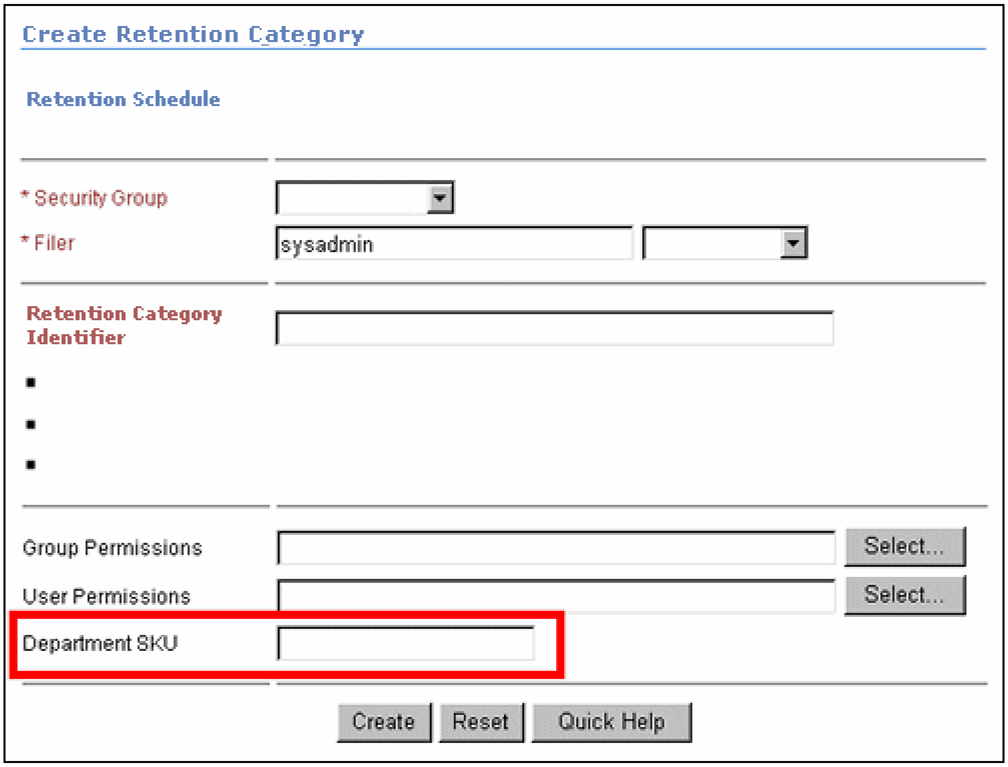
To create a custom retention category metadata field, complete the following steps:

1. Select **Configure—Metadata Sets—Retention Categories** from the Configure Records Management Page (page 7-2).

   The Fields for Metadata Page (page 11-6) is displayed.

2. Click **Create Field**. The Create/Edit Metadata Field Page (page 11-8) is displayed.
3. Click **Add**. The Create/Edit Metadata Field Page (page 11-8) is displayed.
4. Complete the metadata fields as follows:
   a. Type `DeptSKU` in the **Name** box.
   b. In the **Type** list, select **Integer**.
   c. In the **Caption** box, type `Department SKU`.
   d. Set the **Option List** value to **No**.
   e. In the **Required** list, select **No**.
   f. In the **Enabled** list, select **Yes**.
   g. In the **Searchable** list, select **Yes**.
5. Click **OK**.
6. Click **Submit Update**. To view the new field, browse content, and click **Create Retention Category** from the **Actions** menu. The new custom metadata field is displayed.

Figure 11-14 Example Custom Retention Category metadata field



* Filer: sysadmin

As you can see in the figure above, the field “Department SKU” has been added to the Create Retention Category page.

Creating a Custom Folder Metadata Field

This example creates a custom folder metadata field for capturing the DOB (Date of Birth) for a person. All records filed into the folder are based on having the same date of birth, which facilitates destruction of obsolete records in complete blocks of data.

Permissions: The Admin.RecordManager right is required to perform the tasks in this example.This right is assigned by default to the ‘rmaadmin’ role.

To create a custom records folder metadata field, complete the following steps:

1. Select **Configure—Metadata Sets—Records Folders** from the Configure Records Management Page (page 7-2).

   The Fields for Metadata Page (page 11-6) is displayed.

2. Click **Create Field**. The Create/Edit Metadata Field Page (page 11-8) is displayed.

3. Click **Add**. The Create/Edit Metadata Field Page (page 11-8) is displayed.
4. Complete the metadata fields as follows:
   a. In the **Name** box, type **`DOB`**.
   b. In the **Type** list, select **Date**.
   c. In the **Caption** box, type **`Date of Birth`**.
   d. Leave the default value as **No** for the **Option List**.
   e. In the **Required** list, select **Yes**.
   f. In the **Enabled** list, select **Yes**.
   g. In the **Searchable** list, select **Yes**.
5. Click **OK**.
6. Click **Submit Update**. To view the new field, select Browse Content and a retention schedule folder then click **Create Records Folder**. The new custom folder metadata field is displayed.

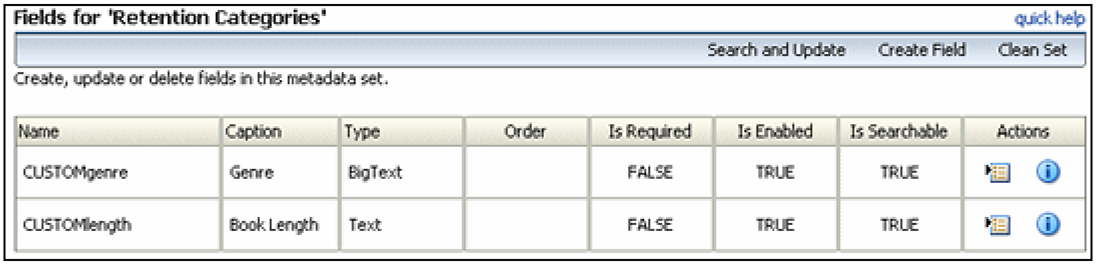
As you can see, the Date of Birth field has been added to the Create Records Folder field, and the Calendar component is automatically associated with the Date Type field. Because the field is required, the field caption “Date of Birth” appears in red text.

CUSTOM METADATA INTERFACE

The following screens are used to set up custom metadata:

- ❖ Fields for Metadata Page (page 11-6)
- ❖ Create/Edit Metadata Field Page (page 11-8)
- ❖ Metadata Information Page (page 11-11)

Fields for Metadata Page



Fields for 'Retention Categories'

Create, update or delete fields in this metadata set.

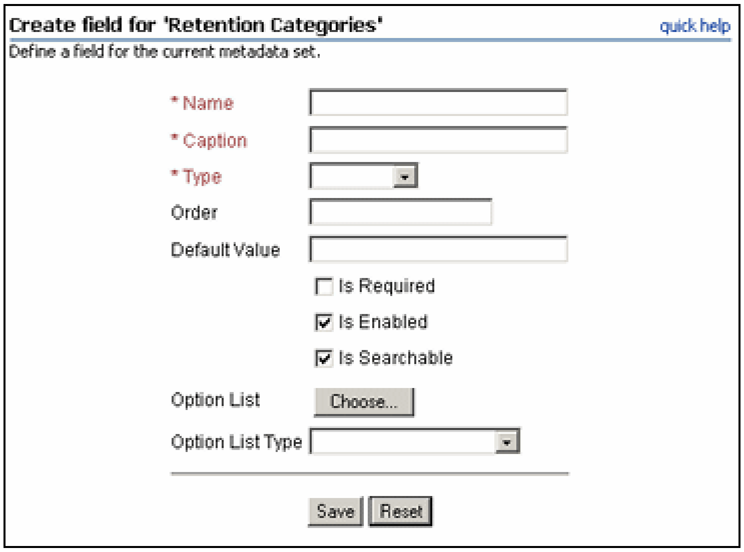
Name	Caption	Type	Order	Is Required	Is Enabled	Is Searchable	Actions
CUSTOMgenre	Genre	BigText		FALSE	TRUE	TRUE	▤ ⓘ
CUSTOMlength	Book Length	Text		FALSE	TRUE	TRUE	▤ ⓘ

This page displays any previously created metadata fields and is used to add new fields. To access this screen click **Configure—Metadata Sets—Retention Categories** or **Configure—Metadata Sets—Records Folders** from the Configure Records Management Page (page 7-2). If you chose to add a Folder Metadata field, the page header is changed.

Feature	**Description**
Search and Update	Opens an Update screen where you can change values in a metadata field. See the Records Manager DoD Edition System Maintenance Guide for details on using this function.
Create Field	Opens the Create/Edit Metadata Field Page (page 11-8) where you can add another field.
Clean Set	❖
Order	Indicate where this field should appear on the pages where it is used.
Default Value	Enter a default value for an **Option List**, **Text**, or **Long Text** field. ❖ Optional. ❖ Maximum characters: 30.
Required	Specify if the custom metadata field is required or optional. Available options: ❖ **No**—Default. The field is optional. ❖ **Yes**—The field is required and users must complete the field.
Enabled	Indicates if the field is enabled on the affected content server pages. Available options: ❖ **No**—Default. The field is not enabled for end-user interaction. ❖ **Yes**—The field is enabled on the user interface and users can interact with the field.

Feature	Description
Searchable	Specify if the field is indexed in the database and therefore searchable by end users. Available options: ❖ **No**—Default. The field cannot be searched by users and does not display on any Search pages. ❖ **Yes**—The field can be searched by users. The field displays on Search and Screening pages.
Option List	If an option list will be used, click the Select button to choose it from the displayed list. An option list must be created and populated before it can be used. See the *Managing Repository Content Guide* for details.
Option List Type	Select the type of option list from the pulldown menu.
Reset button	If you are creating a new custom metadata field, this resets the page to its initial default settings. If you are editing an existing custom metadata field, this returns your original settings.

Create/Edit Metadata Field Page


Create field for 'Retention Categories'

Define a field for the current metadata set.

* Name	
* Caption	
* Type	
Order	
Default Value	

□ Is Required

☑ Is Enabled

☑ Is Searchable

Option List

Option List Type

Permissions: The Admin.RecordManager right is required to use this page. This right is assigned by default to the ‘rmaadmin’ role.

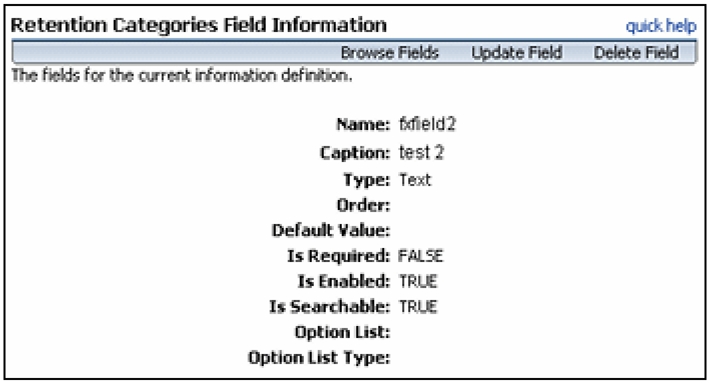
Use this page to create or edit a custom metadata field for a retention category or records folder. To access this page, click Create Field from the Fields for Metadata Page (page 11-6).

Feature	Description
Name	Enter a unique name for the custom category or folder field. This name represents the field name in the database. ❖ Required. ❖ Maximum characters: 30. ❖ Restricted characters: spaces, tabs, line feeds, carriage returns, semi-colon (;) caret (^), question mark (?), colon (:), at-sign (@), ampersand (&), plus sign (+), double-quote ("), pound or hash sign (#), percent sign (%), less than sign (<), asterisk (*), tilde (~), pipe (|), or dash (-).
Caption	Enter a caption for the custom category or folder field. The caption is the field label that displays on the user interface if the field is enabled as such. ❖ Required. ❖ Maximum characters: 30.
Type	Select the data type for the custom category or folder metadata field. ❖ **Text**—(default) Text field of 30 characters. ❖ **Long Text**—Text field of 100 characters. ❖ **Integer**—An integer value ranging from -2^{31} to 2^{31} (-2 billion to +2 billion). Decimal values and commas are not permitted. ❖ **Memo**—Text field of 1000 characters. ❖ **Date**—A date field according to the date format specified in your system settings, such as *dd/mm/yyyy* or *dd/mm/yy* for the English-US locale. Selecting this type puts the Calendar component icon next to the date field.

Feature	Description
Order	Indicate where this field should appear on the pages where it is used.
Default Value	Enter a default value for an **Option List**, **Text**, or **Long Text** field. ❖ Optional. ❖ Maximum characters: 30.
Required	Specify if the custom metadata field is required or optional. Available options: ❖ **No—**Default. The field is optional. ❖ **Yes**—The field is required and users must complete the field.
Enabled	Indicates if the field is enabled on the affected content server pages. Available options: ❖ **No—**Default. The field is not enabled for end-user interaction. ❖ **Yes**—The field is enabled on the user interface and users can interact with the field.
Searchable	Specify if the field is indexed in the database and therefore searchable by end users. Available options: ❖ **No—**Default. The field cannot be searched by users and does not display on any Search pages. ❖ **Yes—**The field can be searched by users. The field displays on Search and Screening pages.
Option List	If an option list will be used, click the Select button to choose it from the displayed list. An option list must be created and populated before it can be used. See the *Managing Repository Content Guide* for details.
Option List Type	Select the type of option list from the pulldown menu.

Feature	Description
Reset button	If you are creating a new custom metadata field, this resets the page to its initial default settings. If you are editing an existing custom metadata field, this returns your original settings.

Metadata Information Page



The fields for the current information definition.

Name: fxfield2
Caption: test 2
Type: Text
Order:
Default Value:
Is Required: FALSE
Is Enabled: TRUE
Is Searchable: TRUE
Option List:
Option List Type:

This page displays information about previously created fields. To access this page, click a field name on the Fields for Metadata Page (page 11-6). You can use this page to browse all created fields, to update the field, or to delete the field.

Chapter

12

CONFIGURING DISPOSITIONS AND FREEZES

OVERVIEW

Disposition actions are used in disposition instructions, which define the sequence of actions to be performed on records and on-record content items during their life cycle. A large number of built-in disposition actions are included, including Cutoff, Destroy, Transfer, Move, Declassify.

Your environment may require disposition actions other than the predefined options. You can set up disposition actions to reflect your organization's specific needs.

Freezing inhibits disposition processing. This can be used to comply with legal or audit requirements. You can define the types of freezes used in your organization, in order to refine the freeze/hold process.

Important: Creating custom disposition actions requires in-depth technical knowledge of Content Server. To define custom disposition actions, contact Consulting Services.

This chapter covers the following topics:

Concepts

- Custom Disposition Actions (page 12-3)
- Freezes (page 12-14)

Tasks

Examples

Interface

Custom Disposition Actions

Custom disposition actions are based on Content Server services, which can be called with specific parameters to define the behavior of the disposition actions. For example, you could create a disposition action to automatically retain the last three revisions of non-record content items using the DELETE_ALL_BUT_LAST_N_REVISIONS_SERVICE service with the 'NumberOfRevisions=3' parameter.

Important: Custom disposition features are available only to users with the Admin.CustomDispositionActions right. By default, this right is not assigned to any of the predefined roles which means you must assign it to a role before this functionality is exposed.

This section covers the following topics:

❖ Managing Dispositions (page 12-3)

❖ Disposition Interface (page 12-6)

❖ Creating a Custom Disposition Action Example (page 12-12)

Managing Dispositions

The following tasks are used when managing dispositions:

❖ Creating or Editing a Custom Disposition Action (page 12-3)

❖ Viewing Custom Disposition Action Information (page 12-5)

❖ Deleting a Custom Disposition Action (page 12-5)

❖ Disabling Custom Disposition Actions (page 12-6)

Creating or Editing a Custom Disposition Action

Use this procedure to create a custom disposition action. For example, you may need a disposition action that retains the last three revisions of a content item.

Important: Creating custom disposition actions requires in-depth technical knowledge of Content Server. Contact Consulting Services to define custom disposition actions.

Permissions: The Admin.CustomDispositionActions right is required to perform this tasks. This right is not assigned by default to any of the predefined roles, which means you must assign it to a role before this functionality is exposed.

1. Select **Configure—Disposition Actions—Custom** from the Configure Records Management Page (page 7-2).

   The Configure Dispositions Page (page 12-6) is displayed.

2. In the Custom Disposition Action area, click **Add**.

   The Create or Edit Disposition Action Page (page 12-7) is displayed.

3. Enter a unique ID for the custom disposition action in the **Action ID** text box.
4. Enter a name for the custom disposition action in the **Action Name** text box.
5. Enter a description for the custom disposition action in the **Brief Description** text box.
6. Enter a group name for the custom disposition action in the **Group Name** text box.
7. Select the service to be used for the custom disposition action from the **Action Service** dropdown list.
8. (Optional) Specify one or more parameters for the selected action service.
9. (Optional) Select or clear any of the check boxes as required.
10. Click **Create**.

    A message is displayed saying that the disposition action was created successfully, with the action information.

11. Click **OK**.

To edit a custom disposition action, complete the following steps:

1. Select **Configure—Disposition Actions—Custom** from the Configure Records Management Page (page 7-2).

   The Configure Dispositions Page (page 12-6) is displayed.

2. Select Edit Action from a disposition's Item Actions popup menu. You can also click on the disposition name and select Edit from the Disposition Action Info Page (page 12-11).

   The Create or Edit Disposition Action Page (page 12-7) is displayed.

3. Make modifications as required, and click **Submit Update** when you finish.

   A message is displayed saying that the disposition action was created successfully, with the action information.

4. Click **OK**.

Viewing Custom Disposition Action Information

Use this procedure to view the information about a custom disposition action.

Permissions: The Admin.CustomDispositionActions right is required to perform this action. This right is not assigned by default to any of the predefined roles, which means you must assign it to a role before this functionality is exposed.

To view the information about a custom disposition action, complete the following steps:

1. Select **Configure—Disposition Actions—Custom** from the Configure Records Management Page (page 7-2).

   The Configure Dispositions Page (page 12-6) is displayed.

2. Click on the disposition name to view.

   The Disposition Action Info Page (page 12-11) is displayed.

3. When you finish viewing the information, click **OK**.

Deleting a Custom Disposition Action

Permissions: The Admin.CustomDispositionActions right is required to delete custom disposition actions. This right is not assigned by default to any of the predefined roles, which means you must assign it to a role before this functionality is exposed.

Important: You can only delete custom disposition actions if they are no longer being used in the disposition instructions for any category. If you attempt to delete a disposition action that is still in use, an error message is displayed.

To delete a custom disposition action, complete the following steps:

1. Select **Configure—Disposition Actions—Custom** from the Configure Records Management Page (page 7-2).

   The Configure Dispositions Page (page 12-6) is displayed.

2. Select **Delete Action** from a disposition's Item **Actions** popup menu. You can also click on the action name and select Delete from the Disposition Action Info Page (page 12-11).

   A message is displayed saying that the disposition action was deleted successfully.

3. Click **OK**.

To delete multiple dispositions, click the checkbox for the dispositions to delete on the Configure Dispositions Page (page 12-6) and select **Delete** from the Table menu.

Disabling Custom Disposition Actions

Permissions: The Admin.CustomDispositionActions right is required to delete custom disposition actions. This right is not assigned by default to any of the predefined roles, which means you must assign it to a role before this functionality is exposed.

To disable a custom disposition action, complete the following steps:

1. Select**Configure—Disposition Actions—Disable** from the Configure Records Management Page (page 7-2).

   The Disposition Actions Configuration Page (page 12-11) is displayed.

2. Select the checkbox next to the actions which should be disabled and made unavailable for use.

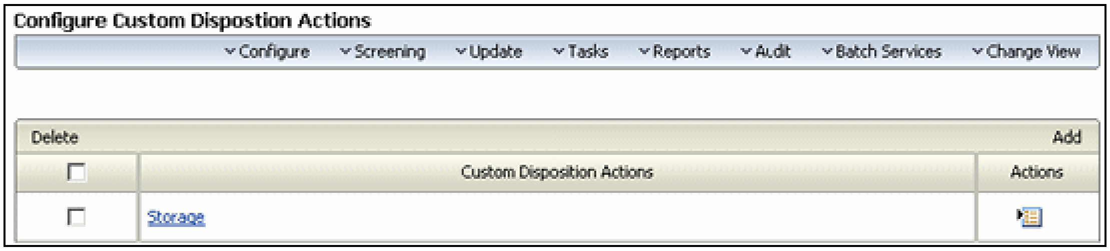
3. Click **Submit Update** when done.

Disposition Interface

The following screens are used when managing dispositions:

- Configure Dispositions Page (page 12-6)
- Create or Edit Disposition Action Page (page 12-7)
- Disposition Action Info Page (page 12-11)

Configure Dispositions Page



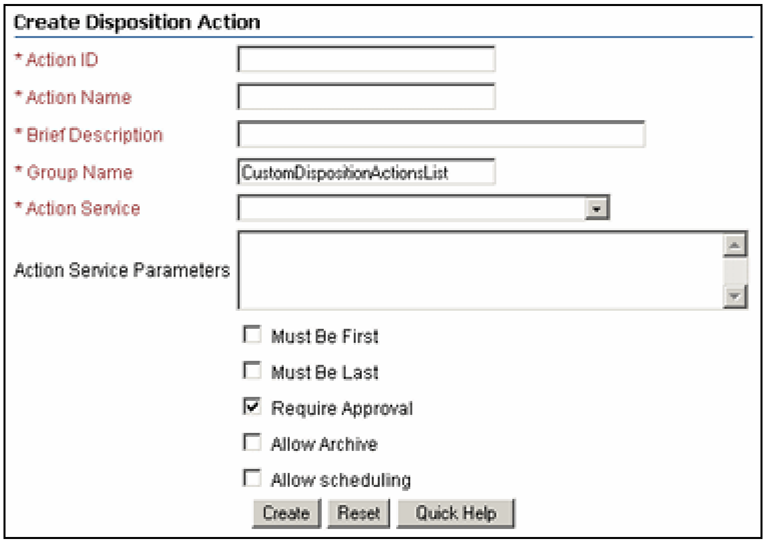
Configure Custom Dispostion Actions

□	Custom Disposition Actions	Actions
□	Storage	

This page is used to access any previously configured dispositions and to add new dispositions. To access this page, select **Configure—Custom Dispositions** from the Configure Records Management Page (page 7-2).

The Configure menu on this page is the same menu used on the Configure Records Management Page (page 7-2). See Configuration Page Menus (page 7-9) for details.

Create or Edit Disposition Action Page



Create Disposition Action

* Action ID

* Action Name

* Brief Description

* Group Name: CustomDispositionActionsList

* Action Service

Action Service Parameters

□ Must Be First

□ Must Be Last

☑ Require Approval

□ Allow Archive

□ Allow scheduling

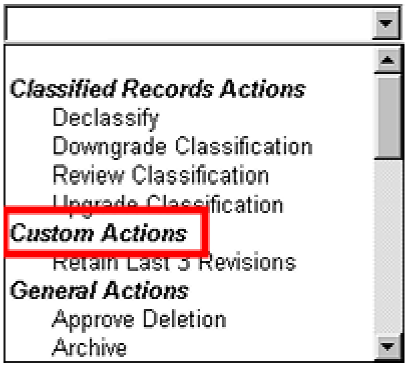
Important: Creating custom disposition actions requires in-depth technical knowledge of Content Server. To define custom disposition actions, contact Consulting Services.

Permissions: The Admin.CustomDispositionActions right is required to use this page. This right is not assigned by default to any of the predefined roles, which means you must assign it to a role before this functionality is exposed.

Use the Create page to define a new custom disposition action. To access this page, click **Add** from the Configure Dispositions Page (page 12-6).

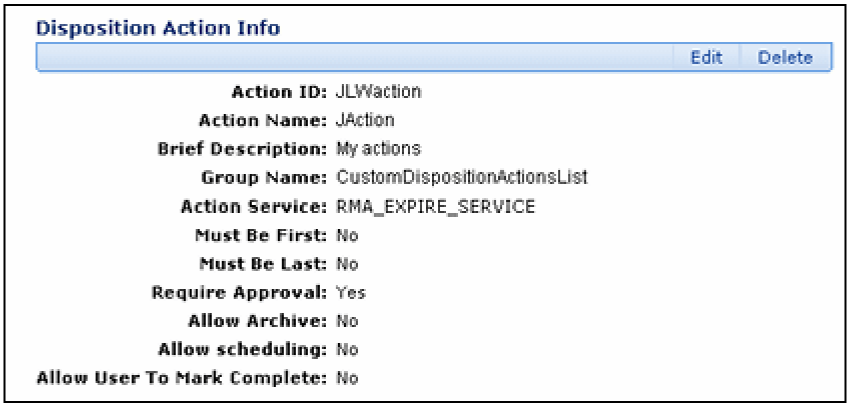
Use the Edit page to modify the properties of an existing custom disposition action. To access this page, select **Edit Action** from the disposition's Item **Actions** menu on the Configure Dispositions Page (page 12-6). You can also click the disposition name and select **Edit** from the Disposition Action Info Page (page 12-11).

Feature	Description
Action ID field	Enter a unique name for the custom disposition action. ❖ Required. ❖ Maximum characters: 30. This field is view-only on the edit page.
Action Name field	Enter a name for the custom disposition action. This is the name that will be shown in the list of available disposition actions. ❖ Required. ❖ Maximum characters: 30.
Brief Description field	Enter a description of the custom disposition action. ❖ Required. ❖ Maximum characters: 100.

Feature	Description
Group Name field	The heading name that the custom disposition action is grouped under in the list of available disposition actions on the Disposition Rule Screen (page 14-25). The default value for this field refers to the UI string label wwOptGroupLabelCustomDispositionActionsList in the <*install_dir*>\custom\RecordsManagement\resources\lang\ww_strings.htm file, which is set to "Custom Actions" by default.  Classified Records Actions Declassify Downgrade Classification Review Classification Upgrade Classification Custom Actions Retain Last 3 Revisions General Actions Approve Deletion Archive To use a different group name than "Custom Actions," modify the string value in the resource file and restart the content server. Do not change the suggested default value in the Group Name field. ❖ Required.
Action Service field	Select the Content Server service to be used for the custom disposition action. **Note:** Contact Consulting Services for assistance with setting up custom disposition actions.
Action Service Parameters field	If required, specify the parameter(s) that should be used for the selected action service. **Note:** Contact Consulting Services for assistance with setting up custom disposition actions.

Feature	Description
Must Be First check box	Select this check box if the custom disposition action can only be used as the first action in a disposition instruction. See Chapter 14 (*Defining Disposition Instructions)* for details.
Must Be Last check box	Select this check box if the custom disposition action can only be used as the last action in a disposition instruction. See Chapter 14 (*Defining Disposition Instructions)*.
Require Approval check box	Clear this check box if the custom disposition action should be performed without sending an e-mail notification for approval. ❖ Default: selected (i.e., approval is required for the disposition action to be performed).
Allow Archive check box	Select this check box if the custom disposition action should be able to archive items affected by the disposition action.
Allow Single Record Approval Only check box	Select this check box if the custom disposition action should be able to process individual items only, not groups.
Allow Scheduling check box	Select this check box if the custom disposition action should be able to be scheduled.
Create button (Create page only)	Creates the new custom disposition action.
Submit Update button (Edit page only)	Submits the edited custom disposition action.
Reset button	If you are creating a new custom disposition action, this resets the page to its initial default settings. If you are editing an existing custom disposition action, this returns your original settings.

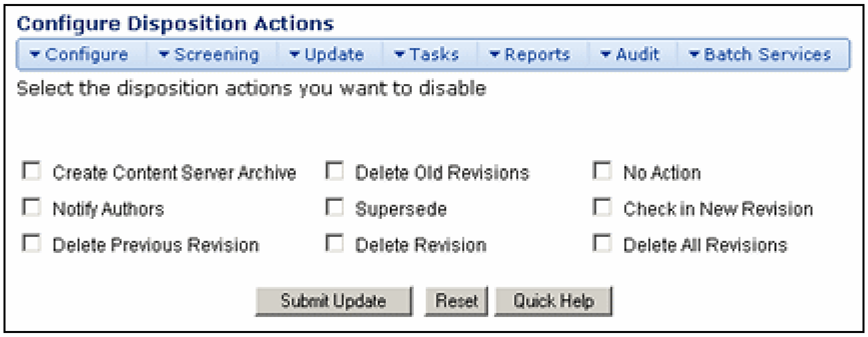
Disposition Action Info Page



Action ID: JLWaction
Action Name: JAction
Brief Description: My actions
Group Name: CustomDispositionActionsList
Action Service: RMA_EXPIRE_SERVICE
Must Be First: No
Must Be Last: No
Require Approval: Yes
Allow Archive: No
Allow scheduling: No
Allow User To Mark Complete: No

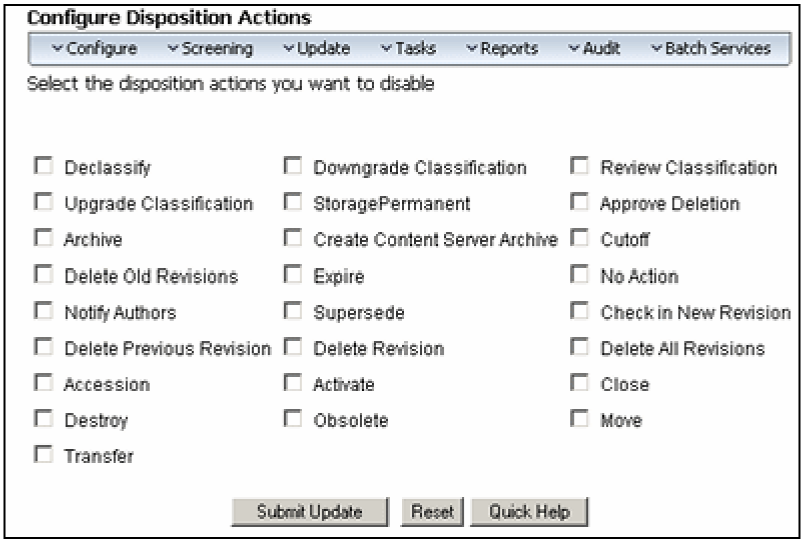
The Disposition Action Info page displays the current characteristics of the selected custom disposition action. To access this page, click on a disposition name on the Configure Dispositions Page (page 12-6).

Disposition Actions Configuration Page



Select the disposition actions you want to disable

□ Create Content Server Archive
□ Notify Authors
□ Delete Previous Revision
□ Delete Old Revisions
□ Supersede
□ Delete Revision
□ No Action
□ Check in New Revision
□ Delete All Revisions



Configure Disposition Actions

Select the disposition actions you want to disable

□ Declassify
□ Upgrade Classification
□ Archive
□ Delete Old Revisions
□ Notify Authors
□ Delete Previous Revision
□ Accession
□ Destroy
□ Transfer
□ Downgrade Classification
□ StoragePermanent
□ Create Content Server Archive
□ Expire
□ Supersede
□ Delete Revision
□ Activate
□ Obsolete
□ Review Classification
□ Approve Deletion
□ Cutoff
□ No Action
□ Check in New Revision
□ Delete All Revisions
□ Close
□ Move

Use this page to set what dispositions actions will be disabled and unavailable for use. To access this pgae, select **Configure—Dispositions—Disable** from the Configure Records Management Page (page 7-2).

Feature	Description
Disposition actions boxes	Displays the actions which can be disabled. These include default actions installed with the system and any dispositions which have been defined.
Submit Update button	Submits your updates.
Reset button	Resets the page to the initial default settings. If you are on an editing page, reset returns your original settings.

Creating a Custom Disposition Action Example

Permissions: The Admin.CustomDispositionActions right is required to perform the tasks in this example. This right is not assigned by default to any of the predefined roles, which means you must assign it to a role before this functionality is exposed.

This example creates a custom disposition action that automatically retains the last three revisions of a non-record content item.

1. Select **Configure—Disposition Actions—Custom** from the Configure Records Management Page (page 7-2).

   The Configure Dispositions Page (page 12-6) is displayed.

2. In the Custom Disposition Action area, click **Add**.

   The Create or Edit Disposition Action Page (page 12-7) is displayed.

3. Complete the metadata fields as follows:

   a. In the **Action ID** field, type `RetainLast3Rev`.

   b. In the **Action Name** field, type `Retain Last 3 Revisions`.

   c. In the **Brief Description** field, type `Only keep the last 3 revisions of a content item`.

   d. In the **Group Name** field, type `Custom`.

   e. From the **Action Service** dropdown list, select DELETE_ALL_BUT_LAST_N_REVISIONS_SERVICE.

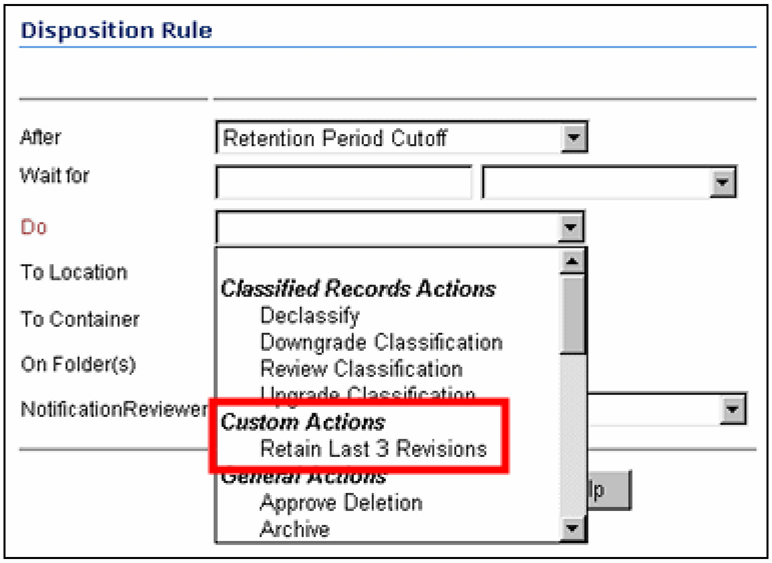
   f. In the **Action Service Parameters** field, type `NumberOfRevisions=3`.

   g. Select the **Require Approval** and **Allow Scheduling** check boxes.

4. Click **Create**.

The newly created disposition action can now be selected from the list of available disposition actions when creating disposition rules.

Figure 12-15 List of available disposition actions in Disposition Rule dialog



Freezes

Note: Freezing is available for record content, non-record content and non-record content that is outside Retention Schedules.

Freezing a record, non-record content item, or records folder inhibits disposition processing for that record, non-record content item, or the records in that folder. This may be necessary to comply with legal or audit requirements (for example, as a result of litigation). In addition, metadata for the folder, record, or item is also frozen.

You can predefine the types of freezes that users can select from a dropdown menu when freezing records or folders. This enables you to better control the freeze/hold process.

Note: If you freeze a non-record content item, *all* revisions of that item are frozen. The revision that you freeze is frozen directly and the other revisions inherit the freeze.

This section covers the following topics:

- ❖ Managing Freezes (page 12-14)
- ❖ Example: Creating a Freeze (page 12-20)
- ❖ Freeze Interface (page 12-21)

Managing Freezes

The following tasks are involved in managing freezes:

- ❖ Creating or Editing a Freeze
- ❖ Searching for Frozen Records, Non-Record Content Items, and Folders
- ❖ Saving a Freeze Screening Report as a File
- ❖ Resending an E-Mail Notification for a Freeze

Creating or Editing a Freeze

Use this procedure to create a freeze that users can select if they want to freeze a record or non-record content item.

Permissions: The Admin.RecordManager right is required to perform this action. This right is assigned by default to the ‘rmaadmin’ role.

1. Select **Configure—Freezes** from the Configure Records Management Page (page 7-2).

   The Freeze Configuration Page (page 12-21) is displayed.

2. In the Freeze area, click **Add**.

   The Create or Edit Freeze Page (page 12-22) is displayed.

3. Select a **Security Group** from the dropdown list.

Note: This field is only displayed if default Content Server security is enabled on the Configure Records Management Page (page 7-2).

4. In the **Filer** field, specify the person who is responsible for creating the freeze. This will normally be the person that is currently logged in, so the default does not generally need to be changed, but you can choose a different user from the dropdown list if required.
5. Specify a **name** for the freeze.
6. (Optional) Specify a **description** for the freeze.
7. (Optional) Specify **group and user permissions** to restrict who has access to the freeze.

Note: These fields are only displayed if ACL-based security is enabled on the Configure Records Management Page (page 7-2).

8. (Optional) Specify the **end date** of the freeze.

Important: The records or non-record content items are not unfrozen automatically at the specified date. This needs to be done manually. This field is used for tracking and documentation purposes only.

9. (Optional) Specify a descriptive text with **instructions for unfreezing** the records or non-record content items.
10. (Optional)Specify if a notification should be sent about the freeze. Notifications are first sent out when the freeze is created.
11. Enter the email address of people to receive the freeze notification and the email address of the person initiating the email.
12. Enter an email message.
13. (Optional)Specify if notification should be periodically re-sent.

14. Select a period of time to wait before re-sending, and the period value (for example, 1 month).
15. Click **Create**.

    A message is displayed saying that the freeze was created successfully, with the freeze information.
16. Click **OK**.

Use the following procedure to edit a freeze:

1. Select **Configure—Freezes** from the Configure Records Management Page (page 7-2).

   The Freeze Configuration Page (page 12-21) is displayed.
2. Select **Edit—Edit Freeze** from a freeze's Item **Actions** popup menu. You can also click on a freeze name and select **Edit—Edit Freeze** from the Page menu.

   The Create or Edit Freeze Page (page 12-22) is displayed.
3. Make modifications as required, and click **Submit Update** when you finish.

   A message is displayed saying that the freeze was updated successfully, with the freeze information.
4. Click **OK**.

Viewing Freeze Information

Permissions: The Admin.RecordManager right is required to view freeze information. This right is assigned by default to the 'rmaadmin' role.

1. Select **Configure—Freezes** from the Configure Records Management Page (page 7-2).

   The Freeze Configuration Page (page 12-21) is displayed.
2. Click on a freeze name to view.

   The Freeze Information Page (page 12-27) is displayed.
3. When you finish viewing the information, click **OK**.

Deleting a Freeze

Permissions: The Admin.RecordManager right is required to perform this action. This right is assigned by default to the ‘rmaadmin’ role. Delete permission (D) for the security group of the freeze is also required. The ‘rmaprivileged’ role does not have this permission by default.

Important: You cannot delete a freeze if that freeze is currently applied to any records and/or folders or non-record content items. If you try, an error message is displayed.

1. Select **Configure—Freezes** from the Configure Records Management Page (page 7-2).

   The Freeze Configuration Page (page 12-21) is displayed.

2. Click on a freeze name to delete.

   The Freeze Information Page (page 12-27) is displayed.

3. Click Delete.

To delete multiple freezes, select the freeze checkbox and click **Delete** on the Table menu on the Freeze Configuration Page (page 12-21).

Unfreezing a Freeze

Use this procedure to unfreeze all folders and records or non-record content items that are currently frozen with a particular freeze.

Permissions: The Admin.RecordManager right is required to perform this action. This right is assigned by default to the ‘rmaadmin’ role.

1. Select **Configure—Freezes** from the Configure Records Management Page (page 7-2).

   The Freeze Configuration Page (page 12-21) is displayed.

2. Select **Edit—Unfreeze** from a freeze’s Item **Actions** popup menu. You can also click on a freeze name and select **Edit—Unfreeze** from the Page menu on the Freeze Information Page (page 12-27).

   The Set Unfreeze Page (page 12-28) is displayed.

3. In the **Unfreeze Reason** field, specify a reason for the unfreeze action.

4. Click **OK**.

A message is displayed saying that all items with the selected freeze have been successfully unfrozen.

5. Click **OK**.

Searching for Frozen Records, Non-Record Content Items, and Folders

Use this procedure to search for records, non-record content items, or folders that are currently frozen with a specific freeze.

Permissions: The Admin.RecordManager and Admin.Screening rights are required to perform this action. These rights are assigned by default to the 'rmaadmin' role.

1. Select **Configure—Freezes** from the Configure Records Management Page (page 7-2).

   The Freeze Configuration Page (page 12-21) is displayed.

2. Click on a freeze name.

   The Freeze Information Page (page 12-27) is displayed.

3. In the **Information** Page menu, click one of the **Screen...** options:

   ❖ **Screen Frozen Content and Records:** Used to display a list of all content items and records that are currently frozen with the selected freeze. The list will not include any frozen content and records that inherited their freeze status from their parent records folder. Note that for non-record content items either this option or the next option produce essentially the same result.

   ❖ **Screen All Frozen Content and Records:** Used to display a list of all records and non-record content items that are currently frozen with the selected freeze. The list includes all frozen records that inherited their freeze status from their parent records folders.

   ❖ **Screen Frozen Folders:** Used to display a list of all folders that are 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 that are 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 Content or Records/Folders Page (page 12-29) is displayed, which lists all records, non-record content, or folders that meet the criteria of the selected screening option.

Saving a Freeze Screening Report as a File

Permissions: The Admin.RecordManager and Admin.Screening rights are required to perform this action. These rights are assigned by default to the ‘rmaadmin’ role.

1. Search for frozen records or folders or non-content items. See Searching for Frozen Records, Non-Record Content Items, and Folders (page 12-18) for details.
2. In the **Information** list on the Frozen Content or Records/Folders Page (page 12-29), click **Save Screening Results**.
3. A file download dialog appears, where you can open or save the file to your hard drive.

Note: The screening report is generated in the report format specified on the Configure Records Management Page (page 7-2).

Note: If the generated report file is in PDF format, it cannot be viewed using Adobe Acrobat 5.*x* or earlier. You need at least version 6.0 of the Acrobat software.

Resending an E-Mail Notification for a Freeze

If you set up e-mail notification for a freeze, the notification e-mail is first sent out when you initially create the freeze (see Creating or Editing a Freeze (page 12-14)). You can elect to periodically send out notifications when you set up a freeze.

Use this procedure to send the e-mail notification about the freeze again (for example, because you want to notify the people involved about a change in the freeze implementation).

Permissions: The Admin.RecordManager right is required to perform this action. This right is assigned by default to the ‘rmaadmin’ role.

1. Select **Configure—Freezes** from the Configure Records Management Page (page 7-2).

   The Freeze Configuration Page (page 12-21) is displayed.
2. Click on a freeze name.

The Freeze Information Page (page 12-27) is displayed.

3. Make modifications to the e-mail properties (recipients, message text) as required.
4. Click **Submit Update** when you finish.

   A message is displayed saying that the freeze was updated successfully, with the freeze information. The notification e-mail has been sent using the e-mail settings of the content server.
5. Click **OK** to return to the Configure Retention Schedule Components page.

Example: Creating a Freeze

This example creates a freeze due to litigation with a company that is valid until 2/20/2010.

Permissions: The Admin.RecordManager right is required to perform the tasks in this example. This right is assigned by default to the ‘rmaadmin’ role.

1. Select **Configure—Freezes** from the Configure Records Management Page (page 7-2).

   The Freeze Configuration Page (page 12-21) is displayed.
2. In the Freeze area, click **Add**.

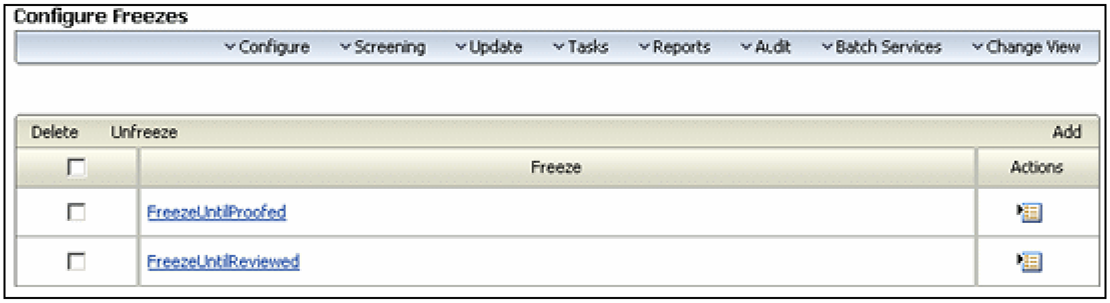
   The Create or Edit Freeze Page (page 12-22) is displayed.
3. In the **Security Group** field, make sure `RecordsGroup` is selected.
4. In the **Filer** field, make sure your own user login is displayed.
5. In the **Freeze Name** field, type `Litigation`.
6. In the **Freeze Description** field, type `Litigation With Company XYZ`.
7. In the **End Date** field, specify 2/20/2010 as the end date, by typing or using the calendar icon.
8. In the **Unfreeze Instructions** field, type `Do not unfreeze the records until the litigation proceedings have been completed`.
9. If required, select the **Send Notification** check box, and provide the e-mail properties (recipients, from-address, and message text).
10. Click **Create** when you finish.

Freeze Interface

The following screens are used when managing freezes;

- Freeze Configuration Page (page 12-21)
- Create or Edit Freeze Page (page 12-22)
- Freeze Information Page (page 12-27)
- Set Unfreeze Page (page 12-28)
- Frozen Content or Records/Folders Page (page 12-29)

Freeze Configuration Page

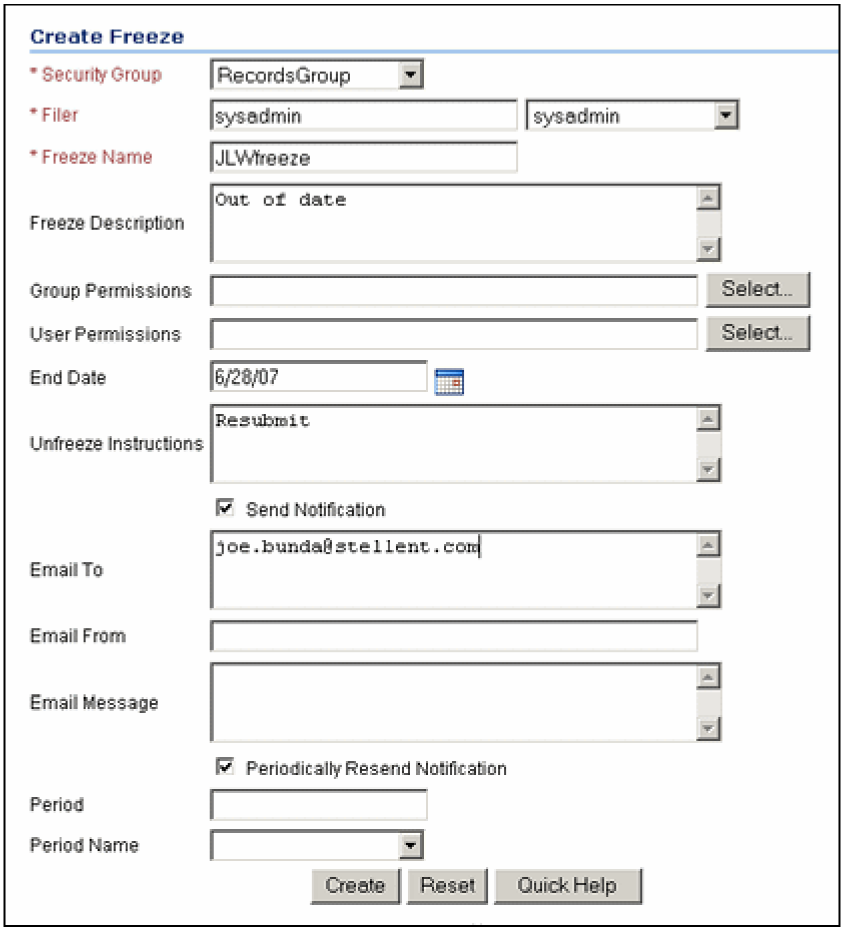


Configure Freezes

□	Freeze	Actions
□	FreezeUntilProofed	
□	FreezeUntilReviewed	

This page is used to add new freezes or to access previously created freezes for editing or deletion. To access this page, select **Configure—Freezes** from the Configure Records Management Page (page 7-2).

Create or Edit Freeze Page



Create Freeze

* Security Group	RecordsGroup ▾	
* Filer	sysadmin	sysadmin ▾
* Freeze Name	JLWfreeze	
Freeze Description	Out of date	
Group Permissions		Select...
User Permissions		Select...
End Date	6/28/07	
Unfreeze Instructions	Resubmit	
	☑ Send Notification	
Email To	joe.bunda@stellent.com	
Email From		
Email Message		
	☑ Periodically Resend Notification	
Period		
Period Name	▾	

Create | Reset | Quick Help

Permissions: The Admin.RecordManager right is required to use this page.

Use the Create page to define a new freeze. To access this page, click **Add** on the Freeze Configuration Page (page 12-21).

Use the Edit page to modify the properties of an existing freeze. To access this page, select **Edit—Edit Freeze** on a freeze's Item Actions popup menu on the Freeze Configuration Page (page 12-21). You can also click a freeze name and select Edit—Edit Freeze on the Page menu on the Freeze Information Page (page 12-27).

Feature	Description
Security Group list	Displays the security group that is allowed access to the freeze. ❖ Required. ❖ Default: RecordsGroup. This field is only displayed if Default Content Server security is enabled on the Configure Records Management Page (page 7-2).
Filer	Displays the person who created the freeze. Select the filer from the options list if you are not the person responsible for creating the freeze. ❖ Required. ❖ Default: Privileged records user that is currently logged in. This field is only displayed if Default Content Server security is enabled on the Configure Records Management Page (page 7-2).
Freeze Name	Enter a name for the freeze. This is the name that will be shown in the list of available freezes. It will also appear in the subject line of an e-mail notification about the freeze. ❖ Required. ❖ Maximum characters: 30. This field is view-only on the edit page.
Freeze Description	Specify a description for the freeze. ❖ Required. ❖ Maximum characters: 1,000.
Group Permissions	Displays any group permissions assigned to the freeze. ❖ Optional. ❖ Maximum characters: 100. This field is only displayed if ACL-based security is enabled on the Configure Records Management Page (page 7-2).

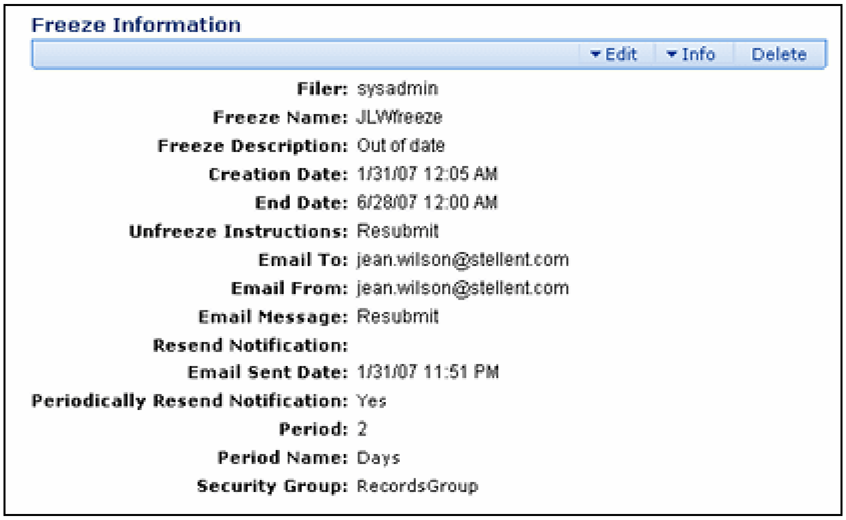
Feature	Description
Select button (Group Permissions)	Opens the Select Alias screen so you can add groups to an access list and set permissions for each group. This field is only displayed if ACL-based security is enabled on the Configure Records Management Page (page 7-2).
User Permissions	Displays users granted access to the freeze. ❖ Optional. ❖ Maximum characters: 100. This field is only displayed if ACL-based security is enabled on the Configure Records Management Page (page 7-2).
Select button (User Permissions)	Opens the Select Users screen so you can add groups to an access list and set permissions for each group. This field is only displayed if ACL-based security is enabled on the Configure Records Management Page (page 7-2).
Creation Date (Edit page only)	The date and time the freeze was created. This field is view-only and is displayed for tracking and documentation purposes.
End Date	(Optional) Specify the date when the freeze ends and when the record or non-record content items should be unfrozen again. Click the calendar icon to choose a date. **Important:** The records or non-record content items are not unfrozen automatically at the specified date. This needs to be done manually. This field is displayed for tracking and documentation purposes only.
Unfreeze Instructions	(Optional) Specify a descriptive text with instructions for unfreezing the records or non-record content items (for example, “Do not unfreeze until...”). This field is displayed for tracking and documentation purposes only. Maximum characters: 1,000.
Unfreeze Reason (Edit page only)	(Optional) Specify a reason for unfreezing all folders and records or non-record content items that are currently frozen with a particular freeze. See Unfreezing a Freeze (page 12-17).

Feature	Description
Send Notification and Periodically Resend Notification check box	Sends an e-mail notification to one or more persons after the freeze is created or edited. For example, you could create a freeze for a lawsuit and notify all people working on that lawsuit that they need to check in any items pertaining to the lawsuit using the associated freeze. The e-mail is (re)sent immediately using the e-mail settings of the content server as soon as you click the Create button (on the Create Freeze page) or the Submit Update button (on the Edit Freeze page). If your e-mail server is not set up correctly, an error message is displayed. The subject line of the e-mail is the freeze name. When an e-mail is sent, a freeze audit information log is checked into the content server. This log contains information about the freeze (freeze name, description, and creation date) as well as information about the e-mail notification that was sent (sender, recipient, message, and send date). E-mail notification cannot be sent if default metadata for checked-in audit logs has not been defined. See the *Records Manager DoD Edition System Maintenance Guide* for details.
Email To	Specify the e-mail address(es) that the notification should be (re)sent to (in the form *user@domain.com*). You cannot use wildcards in the e-mail addresses. To send the notification to multiple recipients, use commas to separate the individual e-mail addresses. Spaces are ignored, so you can insert spaces after each comma if you like. Do not press Enter to put e-mail 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 check box is selected). ❖ Maximum characters: 3,000.

Feature	Description
Email From	Specify the e-mail address of the person who sent the notification (in the form *user@domain.com*). You can only specify one e-mail address. If you leave this field blank, the sender of the e-mail notification (the "From" field in the e-mail) will be the e-mail address of the user who created the freeze or resent the notification (as specified in the user profile). ❖ Optional (if Send Notification check box is selected). ❖ Maximum characters: 100.
Email Message	Specify the body text of the e-mail notification (the actual message)—for example, "A new freeze called 'Legal Case 19403' has been created. Please make sure that you apply this freeze to all documents pertaining to this case." ❖ Required (if Send Notification check box is selected). ❖ Maximum characters: 3,000.
Email Sent Date (Edit page only)	Displays the date and time that the e-mail notification about the freeze was last sent.
Create button (Create page only)	Creates the new freeze.
Submit Update button (Edit page only)	Submits the edited freeze.
Reset button	If you are creating a new freeze, this resets the page to its initial default settings. If you are editing an existing freeze, this returns your original settings.

Security Group list, Filer, Group Permissions, the Select button (Group Permissions), User Permissions, Select button (User Permissions) are only displayed if specific security settings are enabled on the Configure Records Management Page (page 7-2).

Freeze Information Page



Filer:	sysadmin
Freeze Name:	JLWfreeze
Freeze Description:	Out of date
Creation Date:	1/31/07 12:05 AM
End Date:	6/28/07 12:00 AM
Unfreeze Instructions:	Resubmit
Email To:	jean.wilson@stellent.com
Email From:	jean.wilson@stellent.com
Email Message:	Resubmit
Resend Notification:	
Email Sent Date:	1/31/07 11:51 PM
Periodically Resend Notification:	Yes
Period:	2
Period Name:	Days
Security Group:	RecordsGroup

The Freeze Information page displays the characteristics of the selected freeze. To access this page, click on a freeze name on the Freeze Configuration Page (page 12-21).

This page shows the current properties of the selected freeze. The Page menu has the following options:

- ❖ **Edit:** Used to edit the current freeze, unfreeze the freeze, or alter the notification.
- ❖ **Delete:** Used to delete the current freeze.

Important: You cannot delete a freeze if that freeze is currently applied to any records and/or folders or non-record content items. If you try, an error message is displayed.

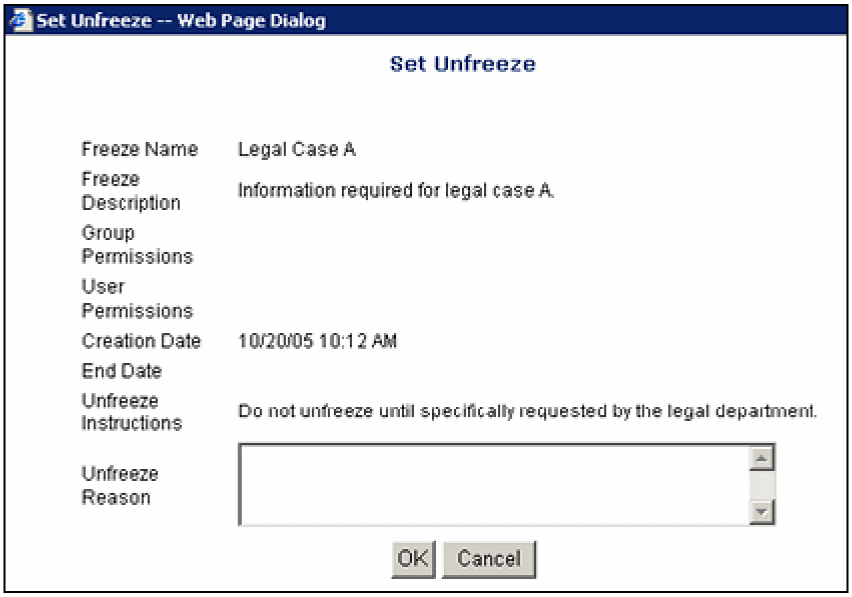
- ❖ **Information:** Used to perform the following searches:
  - **Screen Frozen Content and Records:** Used to display a list (see Frozen Content or Records/Folders Page (page 12-29)) of records and non-record content items that are frozen with the current freeze. The list does not include any frozen records that inherited their freeze status from their parent records folder. See Searching for Frozen Records, Non-Record Content Items, and Folders (page 12-18) for further details.
  - **Screen All Frozen Content and Records:** Used to display a list (see Frozen Content or Records/Folders Page (page 12-29)) of all records and non-record

content items that are frozen with the current freeze. The list also includes all frozen records/non-records that inherited their freeze status from their parent folders. See Searching for Frozen Records, Non-Record Content Items, and Folders (page 12-18) for further details.

- **Screen Frozen Folders:** Used to display a list (see Frozen Content or Records/Folders Page (page 12-29)) of folders that are frozen with the current freeze. The list does not include any frozen folders that inherited their freeze status from their parent folders. See Searching for Frozen Records, Non-Record Content Items, and Folders (page 12-18) for further details.
- **Screen All Frozen Folders:** Used to display a list (see Frozen Content or Records/Folders Page (page 12-29)) of all folders that are frozen with the current freeze. The list includes all frozen folders that inherited their freeze status from their parent folders. See Searching for Frozen Records, Non-Record Content Items, and Folders (page 12-18) for further details.

Permissions: The **Screen...** options are available only if you have the Admin.Screening right.

Set Unfreeze Page


Set Unfreeze -- Web Page Dialog

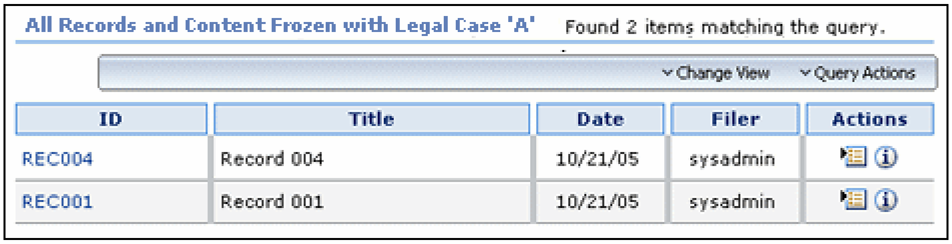
Set Unfreeze

Freeze Name	Legal Case A
Freeze Description	Information required for legal case A.
Group Permissions	
User Permissions	
Creation Date	10/20/05 10:12 AM
End Date	
Unfreeze Instructions	Do not unfreeze until specifically requested by the legal department.
Unfreeze Reason	

Use the Set Unfreeze page to specify a reason for canceling the frozen status of records and non-record content items. To access this page, select **Records Administration—**

Configure Retention Schedule Components from the **Administration** tray. In the Freeze area, select the freeze to be specified, and click **Unfreeze**.

Frozen Content or Records/Folders Page



All Records and Content Frozen with Legal Case 'A' Found 2 items matching the query.

ID	Title	Date	Filer	Actions
REC004	Record 004	10/21/05	sysadmin	☰ ⓘ
REC001	Record 001	10/21/05	sysadmin	☰ ⓘ

Permissions: The Admin.RecordManager right and Admin.Screening right is required to use this page.

The Frozen Content or Records/Folders page displays a list of the records, non-record content items, or folders that are frozen with the current freeze. To access this page, select **Information** then the screening type from a freeze on the Freeze Configuration Page (page 12-21). See Searching for Frozen Records, Non-Record Content Items, and Folders (page 12-18) for more information.

You can also save the screening results as a file, in the report format specified on the Configure Records Management Page (page 7-2).

Note: If the generated report file is in PDF format, it cannot be viewed using Adobe Acrobat 5.*x* or earlier. You need at least version 6.0 of the Acrobat software.

Chapter

13

CONFIGURING RELATED CONTENT (LINKS)

OVERVIEW

Links establish a type of relationship between individual records and managed content items. This may be useful when records and non-record content items are related and need to be considered together, for example:

- A native file (for example, in Word) has several different renditions such as a PDF or thumbnail image, each of which is checked into the content server as a separate content item.
- A native file (for example, in Word) contains a number of embedded images, each of which is checked into the content server as a separate content item.
- A native file (for example, in Word) contains a number of links to other native files (for example, in Word), each of which is checked into the content server as a separate content item.

Note: Links previously created using the RmaLinks component do not carry over if you have installed a newer version of software that uses the Related Content component.

This chapter covers the following topics:

Concepts

- About Related Content (page 13-2)
- Predefined Relationship Types (page 13-3)

- Linking Methods (page 13-7)

Tasks

- Adding or Editing a Custom Relation Type (page 13-10)
- Deleting a Custom Link Type (page 13-11)
- Linking Items (page 13-11)
- Unlinking an Item (page 13-12)

Examples

- Enclosures Custom Link Types Example (page 13-13)
- Renditions Link Example (page 13-15)
- One-Way Cross-Reference Link Example (page 13-15)
- Reciprocal Cross-Reference Link Example (page 13-16)
- Superseded Link Example (page 13-18)
- Supporting Content Link Example (page 13-19)

Interface

- Link Management Interface (page 13-20)

About Related Content

Related content establishes a type of relationship, or link, between individual items. The relationships are based on one of four available Relationship Classes (page 13-8). A number of Predefined Relationship Types (page 13-3) are also provided but you can also add custom relationship types to suit the need of your environment. See Adding or Editing a Custom Relation Type (page 13-10) for details.

Permissions: The Admin.ConfigureLinkTypes right is required to perform these actions.

There are two basic methods of creating relationships between items:

- **Creating a relationship from one existing item to another existing item:** If you create a relationship from an item in the system to another, existing item in the system, you use the search page during the process to access the existing item and link to it. For details see Linking to an Existing Item (page 13-12).

- **Creating a relationship from an existing item to a new item:** If you add a relationship from an item to a new item, you use the content check-in page during the process to create the new item to which you are linking. For details see Linking to a New Item (page 13-11).

Permissions: 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, etc.

Important: When items are deleted, all corresponding relationships are deleted, except in the case when a superseded record is in the midst of disposition processing. A “dangling relationship” exists until such time that the superseded content item completes its disposition processing, then the relationships are deleted.

PREDEFINED RELATIONSHIP TYPES

The following predefined relationship types are available:

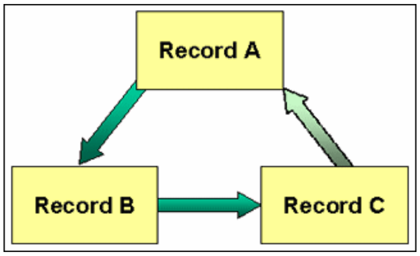
- Renditions (page 13-3), based on the Peer-to-Peer Class (page 13-8)
- Supersedes (page 13-4), based on the Chained List Class (page 13-8)
- Supporting Content (page 13-5), based on the Supporting Content Class (page 13-9)
- Cross-Reference (page 13-6), based on the Cross-Reference Class (page 13-9)

You can also define your own relationship types.

Renditions

The predefined Renditions type is based on the Peer-to-Peer Class (page 13-8). It is typically used to indicate peer relationships between items. Rendition when used in the 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 display 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 13-1 Renditions links



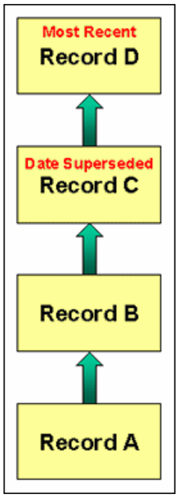
This figure above shows that Record A is linked to Record B, and Record B is linked to Record C. Record C is linked indirectly by association to record A, but it is not actually linked directly to Record A. If the link between Record A and Record B is removed (unlinked, that is), then Record C is no longer linked by association to Record A.

To step through an example of creating this type of link, see Renditions Link Example (page 13-15).

Supersedes

The predefined Supersedes relationship is based on the Chained List Class (page 13-8). It is used when an item, such as a content item that is subject to review, 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 allows you to harness the disposition processing to handle superseded items if you so desire. This type of relationship is created by anyone in the RecordsGroup security group to link an item that supersedes another.

Figure 13-2 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.

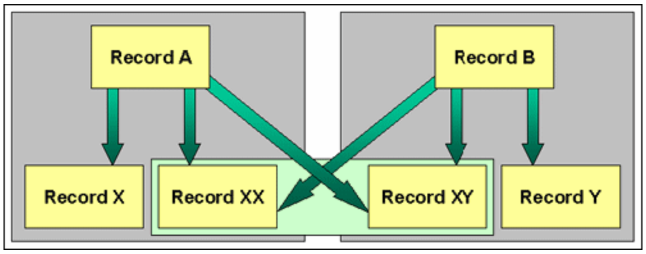
This figure shows Record A was superseded by Record B, which was superseded in turn by Record C, which was superseded by Record D. Record D is the most recent record. The date superseded is set on the previously active record, which in this scenario, is record C. To step through an example of creating this type of relationship, see Superseded Link Example (page 13-18).

Supporting Content

The predefined Supporting Content type is based on the Supporting Content Class (page 13-9). There is one “main” item (the parent) which has a number of subordinate, supporting items (the children). Supporting content links are based on the premise that a supporting content child can have multiple parent items that 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 that support 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. You can also use the supporting content type of relationship for an item that has embedded content. The supporting content relationship is convenient for linking portions of web site 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 that cross 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 13-3 Supporting content links



This figure shows that Records A and B are the only parent records. Record A has child Records X, XX, and XY. Record B has child records Records XX, XY, and Y. Both child records XX and XY have multiple parents, Records A and B. To step through an example of creating this type of link, see Supporting Content Link Example (page 13-19).

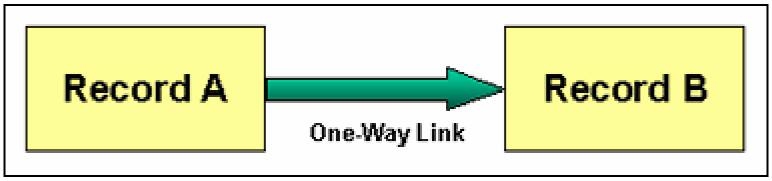
Cross-Reference

The predefined Cross-Reference relationship is based on the Cross-Reference Class (page 13-9). 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 (i.e., going one way only) or bidirectional (or reciprocal; i.e., going both ways).

Unidirectional Links

In this figure, record A is linked to record B. On the content information page for record A, record A indicates a cross-reference relationship to record B. On the content information page for record B, record B indicates it is cross-referenced by a relationship to record A.

Figure 13-4 One direction cross-reference relationship

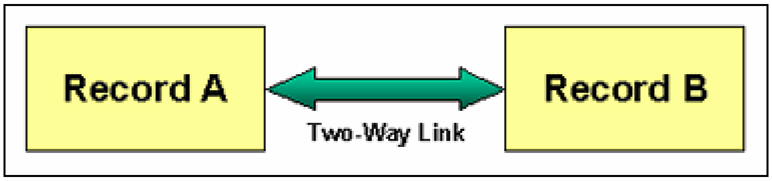


To step through an example of creating this type of relationship, see One-Way Cross-Reference Link Example (page 13-15).

Bidirectional (Reciprocal) Relationships

In the previous figure, record A points to B and vice versa. Record A is cross-referenced to record B, and record B is cross-referenced to record A. When you create a reciprocal relationship from record A to record B, a cross-reference relationship is automatically created from record B to record A.

Figure 13-5 Both directions (reciprocal) cross-reference relationship



To step through an example of creating this type of relationship, see Reciprocal Cross-Reference Link Example (page 13-16).

LINKING METHODS

There are two basic methods of creating relationships between records/non-records:

- **Creating a relationship from one existing item to another existing item:** If you create a relationship from an item in the system to another, existing item in the system, you use the search page during the linking process to access the existing record and link to it. For details see Linking to an Existing Item (page 13-12).
- **Creating a relationship from an existing content item to a new item:** If you add a relationship from an item in the system to a new item, you use the content check-in page during the linking process to create the new item to which you are linking. For details see Linking to a New Item (page 13-11)

Important: When records are deleted, all corresponding relationships are deleted, except in the case when a superseded record is in the midst of disposition processing. A “dangling link” exists until such time that the superseded record completes its disposition processing, then the relationships are deleted.

Relationship Classes

Each relationship type is based on a class definition of the relationship. There are four types of classes:

- Peer-to-Peer Class (page 13-8)
- Chained List Class (page 13-8)
- Supporting Content Class (page 13-9)
- Cross-Reference Class (page 13-9)

Peer-to-Peer Class

The peer-to-peer class represents a relationship between records or content where none of the items is more important than the other. There is no “master” or “parent” content 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 records or content items (m) can have many relationships to other records or content items (n).

Universal Records Management DoD Edition comes with a predefined relationship type based on the peer-to-peer class: the Renditions type (see Renditions (page 13-3)).

Chained List Class

The chained list class represents a relationship between records or content where the individual items are interconnected in series, thus creating a “chain” of linked items. An example would be incremental versions of a record that supersede each other, where you start out with the first version, link the second version, link 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) record or content item that has superseded many (m) records or content items.

The chained list class is comparable to the revisions concept within Content Server, but operates at a different level. Chained lists span multiple records or content items, whereas revision lists are for individual content items only.

DoD Edition comes with a predefined type based on the chained list class: the Supersedes (page 13-4).

Supporting Content Class

The supporting content class represents a relationship between records or content where there is one “main” item (the parent) which has a number of subordinate, supporting items (the children). Typical examples would be documents that contain 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 content server 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 record or content item that has many (m) supporting records or 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.

DoD Edition comes with a predefined type based on the supporting content class: the Supporting Content link type (see Supporting Content (page 13-5)).

Cross-Reference Class

The cross-reference class represents a one-to-one relationship between a pair of records or content items. The relationship is a cross-reference that points a record or content item to another record or 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 that contains a reference to another document, where these documents are linked together.

DoD Edition comes with a predefined type based on the cross-reference class: the Cross-Reference link type (see Cross-Reference (page 13-6)).

Managing Related Content

The following tasks are involved in managing links:

- Adding or Editing a Custom Relation Type (page 13-10)
- Deleting a Custom Link Type (page 13-11)
- Linking Items (page 13-11)
- Unlinking an Item (page 13-12)

Adding or Editing a Custom Relation Type

You must use one of the predefined classes for this task.

Permissions: The Admin.ConfigureLinkTypes right is required to perform this action. This right is assigned by default to the ‘rmaadmin’ role.

1. Select **Configure—Related Content Types** from the Configure Records Management Page (page 7-2).

   The Configure Link Types Page (page 13-20) is displayed.

2. Click **Add Related Content Type**.

   The Add or Edit Related Content Type Page (page 13-22) is displayed.

3. Enter a name in the **Name** box.

4. (Optional) Enter a destination in the **Destination** box.

5. Select a type from the **Class** list. For more information about classes, see Relationship Classes (page 13-8).

6. Click **Add**.

   The new type is added.

Use this procedure to edit the name or destination of a custom type. You are not allowed to edit the class.

1. Select **Configure—Related Content Types** from the Configure Records Management Page (page 7-2).

   The Configure Link Types Page (page 13-20) is displayed.

2. Click **Add Related Content Type**.

   The Add or Edit Related Content Type Page (page 13-22) is displayed.

3. In the **Actions** popup menu for the custom link to edit, click **Edit**.

   The Add or Edit Related Content Type Page (page 13-22) is displayed.

4. If required, edit the name in the **Name** box.

5. If required, enter or edit a destination in the **Destination** box.

6. Click **Submit Update**.

   The type is updated on the Configure Link Types page.

Deleting a Custom Link Type

You cannot delete built-in types (System = "Yes"). If a custom type is in use, you cannot delete it until you remove it from use (see Unlinking an Item (page 13-12) for further details). When you delete a custom type, this deletes the type definition, but does not delete any of the associated records or content items.

Permissions: The Admin.ConfigureLinkTypes right is required to perform this action. This right is assigned by default to the 'rmaadmin' role.

1. Select **Configure—Related Content Types** from the Configure Records Management Page (page 7-2).

   The Configure Link Types Page (page 13-20) is displayed.

2. Select Delete from the **Actions** popup menu for the existing link type to delete.

   You are prompted to confirm the action.

3. Click **OK**.

   The link type is deleted from the Configure Link Types page.

Linking Items

You can link a record to a new record or to an existing record. You can link an existing record in the retention schedule to a new record that you check in, or an existing record that you search for:

- **Link New Item:** Opens the Content Check In Form so you can check in a new record linked to an existing record.
- **Link Existing Item:** Opens the Search page so you can search for the existing records to link to an existing record.

Linking to a New Item

1. Access the existing record from which to link using the method you prefer:
   - Browse the retention schedule and list records within a record category or record folder.
   - Screen Content and Records for the record if you have the records administrator privilege.
   - Search for an existing record to link.

2. From the Retention Schedule, Records Screening Results, or Search Results page, select the relationship type from the item’s **Actions** menu.
3. In the Page menu of the link page, click **Link—Link New Item**. The Content Check In Form is displayed with **Is Record** already enabled for you.
4. Check in the new record to which to link. For more information about how to check in a record and non-record content item, see the *Records Manager DoD Edition User Guide*.

Linking to an Existing Item

1. Access the existing record from which to link using the method you prefer:
   - ❖ Browse the retention schedule and list records within a retention category or record folder using the **List records** link.
   - ❖ Screen Content and Records for the item if you have the records administrator privilege.
   - ❖ Search for an existing record to link.
2. From the Retention Schedule, Records 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 that link type opens.
4. In the menu of the link page, click **Link—Link Existing Item**. The Advanced Search page is displayed.
5. Search for the record to which to link. For information about searching for records, see the *Records Manager DoD Edition User Guide* or *Content Server User Guide*. A search results page is displayed with a Link column added.
6. Select the check box in the **Link** column next to the record or items to which to link.
7. From the Table menu, click **Link—Link Selected Items**. The Link Page for the type of link you created is displayed, listing the record to which the link was established.

Unlinking an Item

Use this procedure to unlink two linked records. There may be some compelling reason for you to remove a link, such as rerouting a link, or using a different type of link altogether.

Important: 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 that appear indented in the Links area of the content information page. The exception to this is a reciprocal cross-reference link; you can unlink from either link page in that case.

1. Navigate to the content information page of the record to unlink.
2. Click on the links that have a (+) to open the respective link page.
3. Select Unlink from the item's **Actions** popup menu..
4. A message is displayed asking you to confirm removal of the link.
5. Click **OK**. The link page is displayed with the formerly linked content item no longer listed.

Link Examples

The following examples demonstrate the use of links:

- Enclosures Custom Link Types Example (page 13-13)
- Renditions Link Example (page 13-15)
- One-Way Cross-Reference Link Example (page 13-15)
- Reciprocal Cross-Reference Link Example (page 13-16)
- Superseded Link Example (page 13-18)
- Supporting Content Link Example (page 13-19)

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. Select **Configure—Related Content Types** from the Configure Records Management Page (page 7-2).

   The Configure Link Types Page (page 13-20) is displayed.

2. Click **Add Related Content Type**.

   The Add or Edit Related Content Type Page (page 13-22) is displayed.

3. Enter the name `Enclosed By` for the link in the **Name** box.

4. Enter `Enclosing Document` in the **Destination** box.

5. Select the **Supporting Content** link type from the **Class** list.

6. Click **Add**.

   The new link type is added to the Configure Link Types page.

7. Click **Add Related Content Type**.

   The Add or Edit Related Content Type Page (page 13-22) is displayed.

8. Enter the name `Enclosure of` for the link in the **Name** box.

9. Enter `Enclosures` in the **Destination** box.

10. Select the **Supporting Content** link type from the **Class** list.

11. Click **Add**.

    The new link type is added to the Configure Link Types page.

The new custom link names are displayed in the Configure Link Types page. The Actions column is now populated with a popup 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 records users in the Records Management 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 (+) displays after the link type in the Content Information page.

An Enclosed By link to other records or content items is present for the current record. If you click the link, a list of the linked items is displayed.

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 you do not have to search or browse for the item. You can quickly access the Content Info link from the Check In Conformation page.

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 is displayed and is initially blank for the new and unlinked item.
3. In the Page menu, click **Link—Link New Item**. The Content Check In Form is displayed with the **Is Record** check box already selected for you.
4. Check in a record called “GIF version” completing only required fields. After you click Check In, the newly checked in and linked item is displayed in the Renditions link page for the record. For any assistance with checking in items, see the *Records Manager DoD Edition User Guide*.
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.

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. Record A (“Disaster Recovery Procedures”) is cross-referenced to record B (“System Backup”).

This example creates a one-way cross-reference between existing items. First you search for the item to which to create links, and then you 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, you can create two items with these titles and then search for them.

1. Browse the retention schedule or search for an existing item to link, for this example, the item called “Disaster Recovery Procedures.” From the Retention Schedule or Search Results page, click the Info icon. The content information page for the item is displayed.
2. In the Links area of the content information page, click **Cross-References** from the listed links. The Cross-References link page for the item is displayed and is initially blank.
3. In the Page menu of the Cross-References Link page, click **Link—Link Existing Item**. The Search Results page for linking the record is displayed.
4. Enter your search criteria, and click **Search**. The Search Results are displayed for you to choose items to link. The title indicates the item from which you are linking. If your search criteria includes the item from which you are linking, that check box is grayed out and unavailable for selection. That prevents linking an item to itself. In the Search Results page for linking, select the check box for the items to have links.
5. In the Page menu of the Search for Links page, click **Link**. The items are linked, and the Cross-References page is displayed again with the ID and Titles of items linked as cross-references. ”
6. Now click the Info icon for a cross-referenced item to open the content information page. Scroll down to the Links area.
7. The item from which we are linking has a (+) appearing after the Cross-Referenced By link.
8. Click the Cross-Referenced By link. The “System Backup: Cross-Referenced By” link page for the item is displayed.
9. 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.

Reciprocal Cross-Reference Link Example

This example creates a two-way link, which means that the linked records point to each other. This example creates a reciprocal cross-reference between existing records. First search for the record to which to create links, and then search for the records to link. Similar screens 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 records with these titles and then search for the records. If you created links for the one-way example, unlink the records before proceeding with this example to view the same results as demonstrated for this example.

1. Browse the retention schedule or search for an existing record to link. From the Retention Schedule or Search Results page, click the Info icon. The content information page for the record is displayed.
2. In the Links area of the content information page, click **Cross-References** from the listed links. The Cross-References link page for the record is displayed and is initially blank.
3. In the Page menu of the Cross-References Link page, click **Link—Link Existing Item**. The Search Results page for linking the record is displayed.
4. Enter your search criteria, and click **Search**. The search results are displayed for you to choose records to link. The title indicates the record you are linking from. If your search criteria includes the record from which you are linking, that check box is grayed out and unavailable for selection. That prevents linking a record to itself. In the Search Results page for linking, select the check box for the records to which to create reciprocal links.
5. In the Page menu of the Search for links page, click **Link—Link Reciprocal**. The records are linked, and the Cross-References page is displayed again with the ID and Titles of records linked as cross-references.
6. Now click the Info icon for the cross-referenced record “System Backup” to open the content information page for the record which was just linked. Scroll down to the Links area. Notice that 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 records.
7. Click the Cross-Referenced By link. The Cross-Referenced By links page is displayed for the record.

You cannot perform any action from the Cross-Referenced By links page with the exception of viewing content information for any listed records. You must unlink the cross-referenced by records from their respective originating cross-references link pages; the same is true of Supported Content By or other “indented” (that is, destination) links.

Superseded Link Example

This example demonstrates creating a superseded link. Because record or content that is subject to review must be kept up-to-date, this example demonstrates superseding items that are subject to review; however, you can supersede items that are not subject to review as well. This example locates an existing item that is subject to review, accesses the supersedes link, and checks in a new item that supersedes the existing one.

Important: The supersedes link is a special type of link in that it allows you to take advantage of disposition processing to handle the superseded records. 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 records; 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 a new record is linked superseded to an existing record, the existing record 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 record, as shown in the screen snippet below:

The current reigning record is always at the top of the list of superseded records. The superseded records are all underneath the current one, and (Superseded) is indicated parenthetically after each superseded record. The superseded records are displayed in the order that the superseding occurred, starting with the first at the bottom of the list.

Of course, you do not have to file records that might be superseded into categories that contain disposition instructions explicit to superseded. Multiple versions of a superseded record can exist similar to multiple versions of a content item; their respective disposition instructions may just involve a retention period and then a destruction.

To step through this example, create a record that is subject to review called “Status Report.” If you have a non-production instance that contains a category that is subject to review with disposition instructions for handling superseded record states, file the record into that category. For assistance, see your administrator. Create another document called “new status report” but do not check it in before the example; we will check it in during the example.

To try out this example:

1. Search for an existing record to link that is subject to review, for this example, a record called “Status Report.”

2. From the search results page, select **Add Link (Supersedes)** from the **Actions** menu of the item to link. The Supersedes link page opens for the existing record called "Status Report."
3. Select **Link—Link New Item** on the Page menu. The Content Check In Form is displayed with the **Is Record** check box already selected for you. Check in the document you created called "New Status Report" as a record that is subject to review into a category whose disposition instructions include actions to handle a superseded state.
4. The Supersedes link page is displayed again with the superseded record and its linked record shown. Notice that the originating record that was superseded is now in the list, with its superior record now listed above it.

   Because the disposition instruction of the record "Status Report" is set to destroy when superseded, the administrator responsible for the record will receive a notification that there is a pending event for the administrator to process (destroying the superseded record).

Supporting Content Link Example

This example demonstrates creating a supporting content link between existing content items and records. The figure below shows some records that will be linked as supporting content. The parent records are "Main HTML Page" and "Annual Corporate Report Brochure."

The "Main HTML Page" parent record has supporting content of the child records "Corporate Logo," "Training Video," and "Training Sound track."

The child record "Corporate Logo" also is used in many other places, including the parent record "Annual Corporate Report Brochure."

1. Search for an existing record to link, for this example, a record called "Main HTML Home Page."
2. From the Search Results page, click **Add Link (Supporting Content)** from the Item **Actions** menu. The Supporting Content link page opens for the existing record called "Main HTML Home Page."
3. In the Page menu, click **Link—Link Existing Item**. The Advanced Search page opens with the ID of the item displayed in the title.
4. Enter your search criteria, and click **Search**. The Search Results page is displayed.
5. Select the item to link as supporting content by selecting the check box for the item.

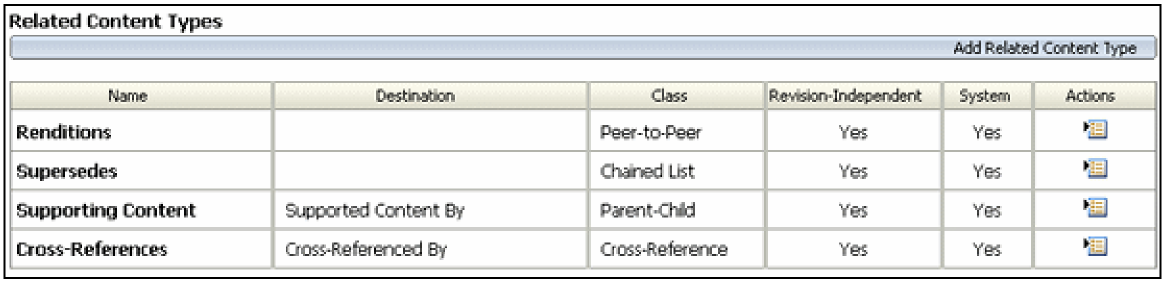
6. In the Page menu, click **Link**. The Supporting Content link page for the record is displayed again, listing the now linked items.
7. Repeat the supporting link process for the parent record “Annual Corporate Report Brochure” and link it to the child record “Corporate Logo,” as shown below.
8. Click the Info icon to access the content information page for the Corporate Logo Image child record. The Supported Content By links indicates there are links present because there is a plus sign.
9. Click the **Supported Content By** link to display the link page for the child record. The Supported Content By indicates the content the record supports. The child record “Corporate Logo” displays its multiple parents.

Link Management Interface

The following screens are used to manage links:

- Configure Link Types Page (page 13-20)
- Add or Edit Related Content Type Page (page 13-22)

Configure Link Types Page



Related Content Types

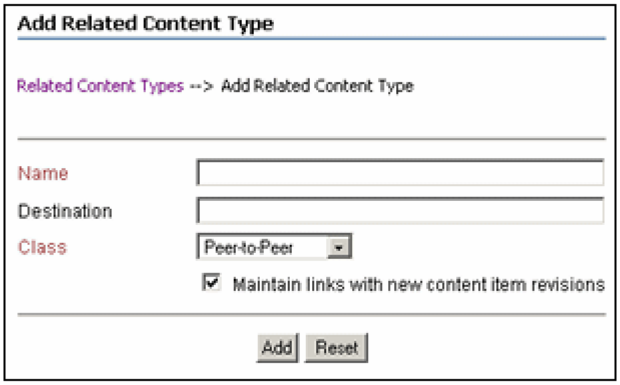
Name	Destination	Class	Revision-Independent	System	Actions
Renditions		Peer-to-Peer	Yes	Yes	▤
Supersedes		Chained List	Yes	Yes	▤
Supporting Content	Supported Content By	Parent-Child	Yes	Yes	▤
Cross-References	Cross-Referenced By	Cross-Reference	Yes	Yes	▤

Permissions: The Admin.ConfigureLinkTypes right is required to use this page. This right is assigned by default to the ‘rmaadmin’ role.

This page is used to view the existing types of links, and to add a custom link name based on one of the predefined link classes. To access this page, select **Configure—Related Content Types** from the Configure Records Management Page (page 7-2).

Feature	**Description**
Name column	The name of the defined link type.
Destination column	The destination of the defined link type, usually a description of the type of linked content item to which the parent points. Destination descriptions are not supported for link types based on the peer-to-peer or chained list link class, so this column is always empty for these link types.
Class column	The link class (see Peer-to-Peer Class (page 13-8)) that the defined link type is based on.
Revision-Independent	Indicates if the relationship is revision independent.
System column	This column contains “Yes” for predefined link types (seePredefined Relationship Types (page 13-3)), and “No” for custom link types.
Actions column	For custom link types (System = “No”), this column contains an Actions icon (▸☰). If you click on this icon, a popup menu appears which enables you to edit or delete the custom link type. For predefined link types (System = “Yes”), this column is always empty. (You cannot edit or delete the predefined link types.)
Action dropdown menu	You can use this dropdown menu to add a new custom link type (see Adding or Editing a Custom Relation Type (page 13-10)).

Add or Edit Related Content Type Page



Add Related Content Type

Related Content Types --> Add Related Content Type

Name
Destination
Class: Peer-to-Peer
☑ Maintain links with new content item revisions

Permissions: The Admin.ConfigureLinkTypes right is required to use these pages. This right is assigned by default to the ‘rmaadmin’ role.

Use the Add page to define your own custom link based on the predefined classes of links. To access this page, click **Add Related Content Type** from the the Configure Link Types Page (page 13-20).

Use the Edit page to modify the properties of an existing custom link type. To access this page, select **Edit** from the related type’s Item Action popup menu..

Feature	**Description**
Name field	Enter the name of your custom link. ❖ Required. ❖ Maximum characters: 50.

Feature	Description
Destination field	This field is available only for link types based on the supporting content or cross-reference link class. You can enter a description of the destination of the custom link type, typically the type of linked item that the parent is pointing to (for example, “Enclosed By” or “Rendition Of”). The destination is displayed on the Configure Link Types Page (page 13-20), and also in the Links area of the content information page of a record or content item. ❖ Optional. ❖ Maximum number of characters: 50.
Class list	Select the link class that the custom link type should be based on. The available link classes are: ❖ (default) Peer-to-Peer Class (page 13-8) ❖ Chained List Class (page 13-8) ❖ Supporting Content Class (page 13-9) ❖ Cross-Reference Class (page 13-9) This field is view-only on the edit page.
Maintain links with new content item revisions	When selected, maintains any links with future revisions of the item.
Add button *(Add Link Type page)*	When selected, the new custom link type is added to the Configure Link Types Page (page 13-20). The links are also available to authorized records users in the Links area of the content information pages and the Actions popup menu on the search results pages.
Submit Update button *(Edit Link Type page)*	When selected, the properties of the custom link type are updated on the Configure Link Types Page (page 13-20)).
Reset button	When selected, the text boxes are cleared and the **Class** dropdown list option reverts to the default.

Chapter

14

DEFINING DISPOSITION INSTRUCTIONS

OVERVIEW

Dispositions are the actions taken on records or non-record content items, usually for items no longer required for conducting current business. Disposition actions for non-record content includes the removal of content not needed for legal reasons or for content that has generally outlasted its usefulness.

Disposition actions for records include activities such as transfer to storage facilities or Federal records centers, transfer of permanent records to the National Archives and Records Administration (NARA), the disposal of temporary records, the replacement of records with updated information, and the adjustment of classifications.

Disposition is the last stage of three stages (creation/receipt, use and maintenance, disposition) in a record's life cycle (see Lifecycle for Records (page 2-6)).

This chapter discusses setting up and administering disposition scheduling. It covers the following topics:

Concepts

Tasks

Examples

Interface

About Dispositions

Dispositions are defined using disposition instructions. A disposition instruction is typically constructed as follows:

1. When a specified triggering event occurs (see Triggering Events (page 14-5)),

2. Wait a specified period of time (the retention period, described in Retention Periods (page 14-7)), if required, and then
3. Perform a specified disposition action (see Disposition Actions (page 14-8)).

A disposition instruction is created within a retention category. All children records folders and records and non-record content items normally inherit dispositions from their parent retention category, but you can apply a disposition rule to a specific records folder only.

Disposition Types

The following types of dispositions are available:

- Event Dispositions (page 14-3)
- Time Dispositions (page 14-4)
- Time-Event Dispositions (page 14-4)

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. Typical examples of an event disposition instruction are “Destroy when obsolete” or, in the case of classified records, “Retain for ten years after declassification.” The disposition actions vary between non-record content and records:

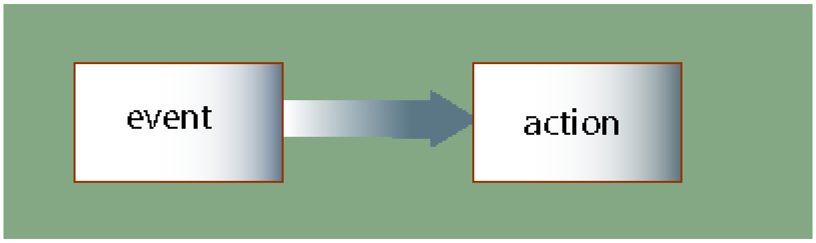
- Records use actions like “destroy” and “retain,” and the states of the record are “obsolete” and “declassified,” respectively.
- Non-records use actions like “Delete revision” and “Delete all revisions.”

To view an example step-by-step procedure for creating an event disposition, see Event Disposition (page 14-17).

Note: If you use records classification (an optional security feature for Records Manager that is certified to comply with the Chapter 4 requirements of the DoD 5015.2 specification), you can set up event disposition 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 (that is, a system-derived) cutoff.

Figure 14-1 Event disposition

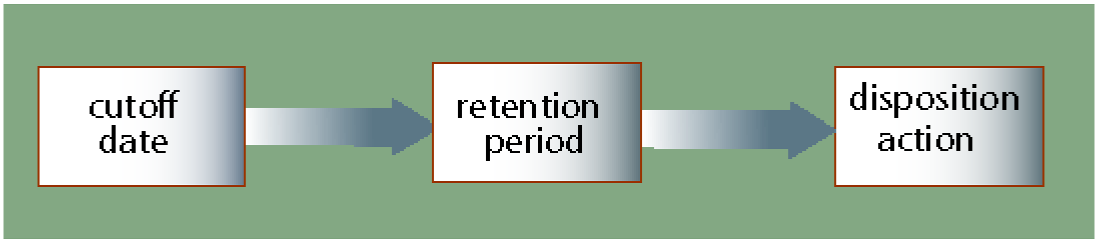


Time Dispositions

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 record or content item. Typical examples of a time disposition instruction are “Cutoff at the end of the (fiscal or calendar) year, retain for three years, then destroy” or, in the case of classified records, “Cut off at declassification, retain for ten years, then destroy.” To view an example step-by-step procedure for creating a time disposition, see Time Disposition (page 14-18).

To summarize, time dispositions have retention periods and explicitly defined cutoffs.

Figure 14-2 Time disposition

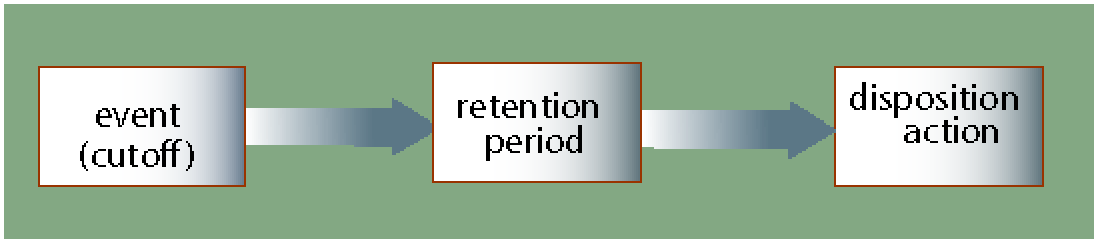


Time-Event Dispositions

A *time-event disposition* is a disposition instruction that begins with a specified triggering event. After the event has transpired, then the folder, record, or non-record 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 (page 14-19).

To summarize, time-event dispositions have retention periods and explicitly defined cutoffs.

Figure 14-3 Time-event disposition



Triggering Events

A disposition instruction is activated when a triggering event occurs. The following built-in triggering events are supported:

Preceding Actions

- **Retention Period Cutoff:** This triggering event cuts off disposition processing and applies a retention period. You can use it for system-derived triggering events that are based on time dispositions or time-event dispositions.
- **Preceding Action:** This triggering event can be used for a disposition rule that is preceded by another rule upon which the subsequent rule depends. For example, one disposition action must be completed before another one can take place.

Record or Content States

- **Activated:** This triggering event is activated when the associated content, records, or records folders have been activated.
- **Cancelled:** This triggering event is activated when the associated records or records folders have been cancelled.
- **Delete Approved:** This triggering event is activated when the associated content, records, or records folders have been approved for deletion.
- **Expired:** This triggering event is activated when the associated records or records folders have been expired.
- **Obsolete:** This triggering event is activated when the associated content, records or records folders have been marked as obsolete.

- **Obsolete and Delete Approved:** This triggering event is activated when the associated records or records folders have been marked as obsolete and have been approved for deletion.
- **Rescinded:** This triggering event is activated when the associated records or records folders have been rescinded (i.e., made void as a result of an enacting authority).
- **Superseded:** This triggering event is activated when the associated content or records have been superseded (i.e., supplanted, or displaced, by records that are more recent or improved).

Note: Records or non-record content items must be linked to be superseded.

- **No Longer Latest Revision:** This triggering event is activated when the associated record or non-record content revisions are no longer the latest revision (i.e., a new revision has been checked into the content server). This trigger allows you 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 triggering event is activated when the associated superseded non-record content or records 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 triggering event is activated when the associated record is the most recent record that is added to a records folder. This allows you to track the activity in a records folder, which can be useful to optimize the usage of records folders based on their activity level. For example, you may decide to delete (or otherwise process) records folders if there has been no activity for a specified period of time.
- **Scheduled declassify date:** This triggering event is activated when the associated records or records folders are scheduled to be declassified on a specific date.

Note: This trigger is available only if the ClassifiedEnhancements component is installed and enabled (see the *Records Manager DoD Edition Installation Guide*).

- **Scheduled downgrade date:** This triggering event is activated when the associated records or records folders are scheduled to be downgraded in their security classification on a specific date.

Note: This trigger is available only if the ClassifiedEnhancements component is installed and enabled (see the *Records Manager DoD Edition Installation Guide*).

❖ **Declassified date:** This triggering event is activated when the associated records or records folders have been declassified on a specific date.

Note: This trigger is available only if the ClassifiedEnhancements component is installed and enabled (see the *Records Manager DoD Edition Installation Guide*).

Indirect Triggers

❖ **Audit Approval:** This triggering event is activated when the associated records or records folders have been approved during an audit (using the built-in “Audit Approval” indirect trigger). This is not available for non-record content.

Custom Triggers

❖ **Custom triggers** are also supported. For more information, see Creating or Editing a Trigger (page 9-6).

RETENTION PERIODS

The retention period is the amount of time that is waited after the triggering event before a disposition action is performed. A number of built-in period units (including calendar years, fiscal quarters, months, and weeks) are available, but you can also create your own (see Creating or Editing a Custom Time Period (page 10-3)).

Examples of retention periods include:

- 5 calendar years
- 2 fiscal quarters
- 6 months
- 4 weeks

Note: For record categories, you can specify a retention period only for the Retention Period Cutoff and Preceding Action triggering events. For non-record categories, you can specify a retention period for all triggering events. This enables you to create disposition rules for non-record content such as “Delete all old revisions three months after the last new revision was checked in.”

DISPOSITION ACTIONS

A disposition action defines what will happen after Triggering Events (page 14-5) occur and Retention Periods (page 14-7), if any, have passed. DoD Edition supports the following built-in disposition actions:

Note: In addition to the built-in disposition actions below, you can define custom disposition actions (see Custom Disposition Actions (page 12-3)).

Important: DoD Edition does not perform the action itself; rather, it sends an e-mail notification to the person responsible for carrying out the action.

General Actions

- **Archive:** This disposition action indicates it is time to archive content, records, or record folders.
- **Create Content Server Archive:** This disposition action indicates it is time to create a Content Server archive that contains the affected records or non-record content with their metadata. This archive can be processed further using the Archiver utility.
- **Cutoff:** This disposition action indicates it is time to cut off content, records, or record folders. Cutoff refers to changing the status of records to allow further processing.
- **Delete Old Revisions:** This disposition action indicates it is time to delete all revisions prior to 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 revisions 1 through 4 are marked for deletion.
    - 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.
- **Move:** This disposition action indicates it is time to move content and records and metadata out of the records management system.
- **No Action:** This disposition action indicates there is no action to take at this time. This action usually found mid-disposition. A No Action action acknowledges that a disposition milestone has passed, and the next step in the disposition begins processing.
- **Notify Authors:** This disposition action indicates it is time to notify the author of the affected category that disposition actions are due for the category.

- **Obsolete:** This disposition action indicates it is time to mark content or records as obsolete.
- **Supersede:** This disposition action indicates it is time to supersede a record or non-record content item by another content item.
- **Transfer:** This disposition action indicates it is time to transfer content or records from one location to another, but does not transfer the legal and physical custody (as with accession).

Non-Records Actions

- **Checkin New Revision:** This disposition action indicates it is time to take the latest revision of the affected content items and check a copy of this revision into the content server 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.
- **Delete Previous Revision:** This disposition action indicates it is time to delete the revision prior to 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 disposition 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.
- **Delete All Revisions:** This disposition action indicates it is time to delete the content item revision that triggered the disposition action as well as 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 from the content server 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.

Record Actions

- **Accession:** This disposition action indicates it is time to transfer physical and legal custody of records and document materials to an archival institution such as NARA.
- **Activate:** This disposition action indicates it is time to activate records folders or records.
- **Approve Deletion:** This disposition action indicates it is time to approve records or record folders for deletion.
- **Close:** This disposition action indicates it is time to close records folders.
- **Destroy:** This disposition action indicates it is time to destroy records folders or records.
- **Expire:** This disposition action indicates it is time to expire records or record folders.

In addition to the built-in disposition actions listed above, you can also define your own disposition actions to reflect your organization's specific records management needs.

Classified Records Actions

- **Declassify:** This disposition action indicates it is time to declassify a record.
- **Downgrade Classification:** This disposition action indicates it is time to lower the security classification of a record to the next lower security classification in the hierarchy.
- **Review Classification:** This disposition action indicates it is time to review the security classification status of a record.
- **Upgrade Classification**: This disposition action indicates it is time to increase the security classification of a record to the next higher security classification in the hierarchy.

Note: These four disposition actions are available only if the ClassifiedEnhancements component is installed and enabled. See the *Records Manager DoD Edition Installation Guide* for details.

Cutoff Guidelines

In most cases, a retention period does not start until a triggering event is set to “cut off.” The length of the retention period determines when to cut off a non-record content item, category, folder, or record and at what interval to perform a cutoff. Use the following guidelines to help you determine when you should cut off and apply retention periods:

You can only specify retention periods for triggers for non-record content items if the `AllowRetentionPeriodWithCutoff` flag is enabled. This is disabled by default.

Time Retention Periods

Records and non-record 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 records.

When a record or non-record 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.

Time-Event Retention Periods

On the date the event or action is completed, perform the cutoff, then apply the retention period.

Disposition Precedence

Records filed into multiple folders that reside in different categories are managed based on the longest time disposition.

When a record has been filed into multiple folders that belong to disparate retention categories, the record is subject to multiple disposition processing schedules. In the event of this scenario, the longest retention period prevails; however, the record is processed by disposition instructions that belong in two or more categories. The following scenario describes a disposition processing precedence.

A record 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 4/1/07	Close after 3/1/07
Archive on 4/10/07	Expire after 4/5/07
Destroy on 4/12/07	Destroy on 4/20/14

The instructions are processed in a staggered order:

1. On 3/1/07, the record will be cutoff with its cutoff date and Folder 2 will be closed.
2. On 4/1/07, the record will be expired and the expiration date will be added to the record (viewable on the content information page).
3. On 4/5/07, the record will not be expired again, so the expiration date is not updated.
4. On 4/10/07, the record and Folder 1 will be archived.
5. On 4/12/07, the pointer to the record is removed from Folder 1 by an update to the record information. The record pointer still exists to Folder 2. The records are not actually filed into a folder, but are "pointed" to the folder.
6. On 4/20/14, the record under Folder 2 will finally be destroyed, as the record is not being held by any remaining pointers.

MANAGING DISPOSITIONS

The following tasks are involved in managing dispositions:

- Enabling or Disabling User-Friendly Captions (page 14-12)
- Creating or Editing a Disposition Rule (page 14-13)
- Viewing Disposition Information (page 14-15)
- Deleting a Disposition Rule (page 14-16)

Enabling or Disabling User-Friendly Captions

You can enable and disable user-friendly captions at any time. This setting also affects the query strings in the Criteria boxes of the Screening pages.

Permissions: The Admin.RecordManager right is required to perform this action. This right is assigned by default to the ‘rmaadmin’ role.

1. Select **Configure Records Management** from the **Administration** tray.

   The Configure Records Management Page (page 7-2) is displayed.
2. Select the **User-Friendly Disposition** check box.
3. Click **Submit Update**. A message is displayed saying that configuration was successful.
4. Click **OK**.

Use this procedure to disable user-friendly captions.

1. Select **Configure Records Management** from the **Administration** tray.

   The Configure Records Management Page (page 7-2) is displayed.
2. Clear the **User-Friendly Disposition** check box.
3. Click **Submit Update**. A message is displayed saying that configuration was successful.
4. Click **OK**.

Creating or Editing a Disposition Rule

A disposition rule applies to all non-record content, records, and record folders in a category by default. You can also create a disposition rule that applies only to a specific records folder. This is a general navigational procedure; to view example procedures for specific types of dispositions, see the Disposition Examples (page 14-16).

Permissions: The Category.Create right is required to perform this action. This right is assigned by default to the ‘rmaadmin’ role.

1. Open the **Browse Content** tray, and click the **Retention Schedules** link. The Exploring Series “Retention Schedule” page is displayed.
2. Navigate to the appropriate retention category.
3. In the row for the retention category, select **Edit—Edit Disposition** from the Item **Actions** popup menu. You can also click the item’s Info icon and select **Edit—Edit Disposition** from the Page menu of the Disposition Information Page (page 14-28).

The (initially blank if creating a disposition) Disposition Instructions Page (page 14-24) is displayed.

4. In the Disposition Instructions area, click **Add**.

   The Disposition Rule Screen (page 14-25) is displayed.

5. Choose the disposition rule's triggering event from the **Triggering Event (After)** list.

6. If the disposition rule has a retention period, enter an integer value in the **Retention Period (Wait for)** box and select the corresponding period from the **Retention Period** list.

7. Select an action for the rule from the **Disposition Action (Do)** list.

8. (Optional) If the disposition action is an option like archive, move, or transfer, enter a description of the location in the **Destination Location (To Location)** text box.

9. (Optional) If the destination location has an associated container, enter a description of the container in the **Destination Container (To Container)** text box.

10. (Optional) If the disposition instruction applies only to a specific records folder, select the records folder from the **Apply to Records Folder (On folder(s))** list. Otherwise, allow the instruction to apply to all records folders within a category.

11. (Optional) If you want a user to review the e-mail notifications triggered by the disposition rule other than the category author, specify that user in the **Notification Reviewer** field by entering the user name or selecting a user from the dropdown list next to the field. If you do not specify a user in this field, only the category author is notified of events triggered by the disposition rule. If you do specify a user, it depends on your system configuration who will receive e-mail notifications: both the specified user and the category author (= default) or the specified user only.

12. Click **OK**. The rule displays in the **Disposition Instructions** box. If the disposition instructions require defining multiple rules, repeat steps 4 through 12 for each rule.

13. 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.

14. Click **Submit Update**. The successfully updated dispositions message is displayed, with the disposition information.

15. Click **OK**.

Use this procedure to edit a disposition rule within the disposition instructions for a retention category.

Permissions: The Category.Edit right is required to perform this action. This right is assigned by default to the ‘rmaadmin’ role.

To edit a disposition rule, complete the following steps:

1. Open the **Browse Content** tray, and click the **Retention Schedules** link. The Exploring Series “Retention Schedule” page is displayed.
2. Navigate to the appropriate retention category.
3. Select **Edit—Edit Disposition** from the item’s **Actions** menu. You can also click the Info icon and display the Disposition Information Page (page 14-28) and select **Edit—Edit Disposition** from the Page menu.

   The Disposition Instructions Page (page 14-24) is displayed.
4. In the Disposition Instructions box, select the rule to edit, and click the edit icon (✏).

   The Disposition Rule Screen (page 14-25) is displayed.
5. Make your changes to the rule, and click **OK**. The Disposition Rule screen closes.
6. Click **Submit Update**. The successfully updated dispositions message is displayed, with the disposition information.
7. Click **OK**.

Viewing Disposition Information

Permissions: The Category.Read right is required to perform this action. By default, this right is assigned to all predefined roles.

1. Open the **Browse Content** tray, and click the **Retention Schedules** link. The Exploring Series “Retention Schedule” page is displayed.
2. Navigate to the appropriate retention category.
3. In the row for the retention category, click the Info icon.

   The Disposition Information Page (page 14-28) is displayed.
4. When you finish viewing the disposition information, click **OK**.

Deleting a Disposition Rule

Use this procedure to delete a disposition rule from the disposition instructions within a category, or delete the entire set of disposition instructions.

Permissions: The Category.Delete right is required to perform this action. This right is assigned by default to the 'rmaadmin' role.

1. Open the **Browse Content** tray and click the **Retention Schedules** link. The Exploring Series "Retention Schedule" page is displayed.
2. Navigate to the appropriate retention category.
3. In the row for the retention category, click **Edit—Edit Disposition**.

   The Disposition Instructions Page (page 14-24) is displayed.
4. Select the rule to delete and click the Delete icon (✖). The rule is deleted from the list. Repeat for each rule to delete.
5. Click **Submit Update**. The successfully updated dispositions message is displayed.
6. Click **OK**.

Disposition Examples

This section includes the following disposition examples:

- Event Disposition (page 14-17)
- Simple Time/Event Disposition (page 14-17)
- Time Disposition (page 14-18)
- Time-Event Disposition (page 14-19)
- Disposition Rules for Specific Folders (page 14-20)
- Conditional ("Or") Disposition (page 14-21)
- Multi-Phased Disposition (page 14-22)

Note: All of the examples in this section use the default (i.e., non user-friendly) disposition captions.

Event Disposition

This example creates an event disposition instruction that destroys records after an event. The event is the records become obsolete. The disposition action is to destroy the records. 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, select **Edit—Edit Disposition** from the item's **Actions** menu. You can also click the Info icon and select **Edit—Edit Disposition** from the Page menu on the Retention Category Information Page (page 8-48).

   The (initially blank) Disposition Information Page (page 14-28) is displayed.
3. In the Disposition Instructions area, click **Add**.

   The Disposition Rule Screen (page 14-25) is displayed.
4. In the **Triggering Event** list, select the **Obsolete** option.
5. In the **Disposition Action** list, select the **Destroy** option.
6. Click **OK**. The disposition rule is displayed in the **Disposition Instructions** box.
7. Click **Submit Update**. The successfully updated disposition message is displayed.

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, select **Edit—Edit Disposition** from the item's **Actions** menu. You can also click the Info icon and select **Edit—Edit Disposition** from the Page menu on the Retention Category Information Page (page 8-48).

   The Disposition Instructions Page (page 14-24) is displayed.
3. In the Disposition Instructions area, click **Add**.

   The Disposition Rule Screen (page 14-25) is displayed.
4. In the **Triggering Event** list, select the **No Longer Latest Revision** option. The Retention Period field becomes available.

5. In the **Retention Period** fields, enter `1` in the text box and select the **Weeks** period unit from the Retention Period list.
6. In the **Disposition Action** list, select the **Notify Authors** option.
7. Click **OK**. The disposition rule is displayed in the **Disposition Instructions** box.
8. Click **Submit Update**. The successfully updated dispositions message is displayed.

Time Disposition

This example demonstrates creating a time disposition with a retention period and a final disposition of destroying records. There is a predictable event trigger that commences 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, select **Edit—Edit Disposition** from the item's **Actions** menu. You can also click the Info icon and select **Edit—Edit Disposition** from the Page menu on the Retention Category Information Page (page 8-48).

   The Disposition Instructions Page (page 14-24) is displayed.
3. In the Disposition Instructions area, click **Add**.

   The Disposition Rule Screen (page 14-25) is displayed.
4. In the **Triggering Event** list, select the **Retention Period Cutoff** option. The Retention Period field becomes available.
5. In the **Retention Period** fields, enter `3` in the text box and select the **Fiscal Years** period unit from 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**. The successfully updated dispositions message is displayed.

Notice that this disposition uses a System-derived triggering event. System-derived means that in this example, once the record becomes obsolete, it is automatically cut off at the end of the fiscal year, and then the retention period begins.

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 in that you cannot predict the exact time that the event might occur, but when it does, the disposition processing begins. A time-event disposition also makes use of a built-in or custom trigger that you define to suit your needs. When the event occurs, you enter the activation date for the custom trigger, if applicable.

This example creates an event disposition instruction that destroys records 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 records.

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, select **Edit—Edit Disposition** from the item’s **Actions** menu. You can also click the Info icon and select **Edit—Edit Disposition** from the Page menu on the Retention Category Information Page (page 8-48).

   The Disposition Instructions Page (page 14-24) is displayed.
3. In the Disposition Instructions area, click **Add**.

   The Disposition Rule Screen (page 14-25) is displayed.
4. Define the first disposition rule:
   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 that the rule prefaced by a preceding action is indented with an ellipsis.

6. Click **Submit Update**. The successfully updated dispositions message is displayed.

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.

- Records folder 1: Event trigger is Program ABC cancelled.
- Records folder 2: Event trigger is Program BBC expired.
- Records folder 3: Event trigger is Program CDB rescinded.

This example requires creating three records 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, select **Edit—Edit Disposition** from the item's **Actions** menu. You can also click the Info icon and select **Edit—Edit Disposition** from the Page menu on the Retention Category Information Page (page 8-48).

   The Disposition Instructions Page (page 14-24) is displayed.
3. In the Disposition Instructions area, click **Add**.

   The Disposition Rule Screen (page 14-25) is displayed.
4. Define the first disposition rule for records folder 1:

   a. In the **Triggering Event** list, select the custom trigger you created for the folder. In this example, it is "Program ABC Canceled."

   b. In the **Disposition Action** list, select the **Destroy** action.

   c. In the **Apply to Records Folder** list, select the folder which will have the rule applied. In this example, the records folder is "Folder 1."

   d. Click **OK**. The rule is displayed in the Disposition Instructions box.
5. Define the second rule for records folder 2:

   a. Click **Add** to add another rule.

   b. In the **Triggering Event** list, select the custom trigger you created for the folder. In this example, it is “Program BBC Expired.”

   c. In the **Disposition Action** list, select the **Destroy** action.

   d. In the **Apply to Records Folder** list, select the folder which will have the rule applied. In this example, the records folder is “Folder 2.”

   e. Click **OK**. The rule is displayed in the Disposition Instructions box.

6. Define the second rule for records folder 3:

   a. Click **Add** to add another rule.

   b. In the **Triggering Event** list, select the custom trigger you created for the folder. In this example, it is “Program CDB Rescinded.”

   c. In the **Disposition Action** list, select the **Destroy** action.

   d. In the **Apply to Records Folder** list, select the folder which will have the rule applied. In this example, the records folder is “Folder 3.”

   e. Click **OK**. The rule is displayed in the Disposition Instructions box.

7. Click **Submit Update**. The successfully updated dispositions message is displayed. Notice that there are rules drawn between the multiple instructions.

Conditional (“Or”) Disposition

This example demonstrates creating a disposition for an instruction that has conditional requirements. Multiple rules are created and exist in parallel, and whichever rule meets the criteria at the appropriate time is the rule that is applied to the associated records. This example makes use of the built-in “Audit Approval” indirect trigger. The instructions are to destroy after an audit is conducted and approved, or when the records become three years of age; whichever event occurs first is the action that disposes of the records.

Disposition Instructions: Destroy after an audit, or when records are 3 years old, whichever is sooner.

1. Navigate to the appropriate category.

2. In the row for the retention category, select **Edit—Edit Disposition** from the item’s **Actions** menu. You can also click the Info icon and select **Edit—Edit Disposition** from the Page menu on the Retention Category Information Page (page 8-48).

   The Disposition Instructions Page (page 14-24) is displayed.

3. In the Disposition Instructions area, click **Add**.

   The Disposition Rule Screen (page 14-25) is displayed.

4. Define the disposition rule for retaining the records until the desired age:
    a. In the **Triggering Event** list, select the **Retention Period Cutoff** option.
    b. In the **Retention Period** controls, enter 3 and select **Calendar Years**.
    c. In the **Disposition Action** list, select the **Destroy** option.
    d. Click **OK**. The rules are displayed in the Disposition Instructions box.
5. Define the disposition rule for the audit:
    a. Click **Add** to add another rule.
    b. In the **Triggering Event** list, select the **Audit Approval** option.
    c. In the **Disposition Action** list, select the **Destroy** option.
    d. Click **OK**. The rule is displayed in the Disposition Instructions box.
6. Click **Submit Update**. The successfully updated dispositions message is displayed. Notice that there are rules drawn between the multiple instructions.

The system performs the cutoff automatically for you because System-Derived indicates "Yes," the disposition action is derived by the system. Manual intervention for cutting off folders is not required in this example.

Multi-Phased Disposition

This example demonstrates defining a disposition instruction that has more phases than is typical in a disposition instruction. This example contains multiple disposition actions: move, transfer, and accession. A "move" disposition action does not transfer the legal responsibility of records, whereas a "transfer" disposition action does transfer both legal responsibility and physical location of records.

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, select **Edit—Edit Disposition** from the item's **Actions** menu. You can also click the Info icon and select **Edit—Edit Disposition** from the Page menu on the Retention Category Information Page (page 8-48).

    The Disposition Instructions Page (page 14-24) is displayed.
3. In the Disposition Instructions area, click **Add**.

    The Disposition Rule Screen (page 14-25) is displayed.

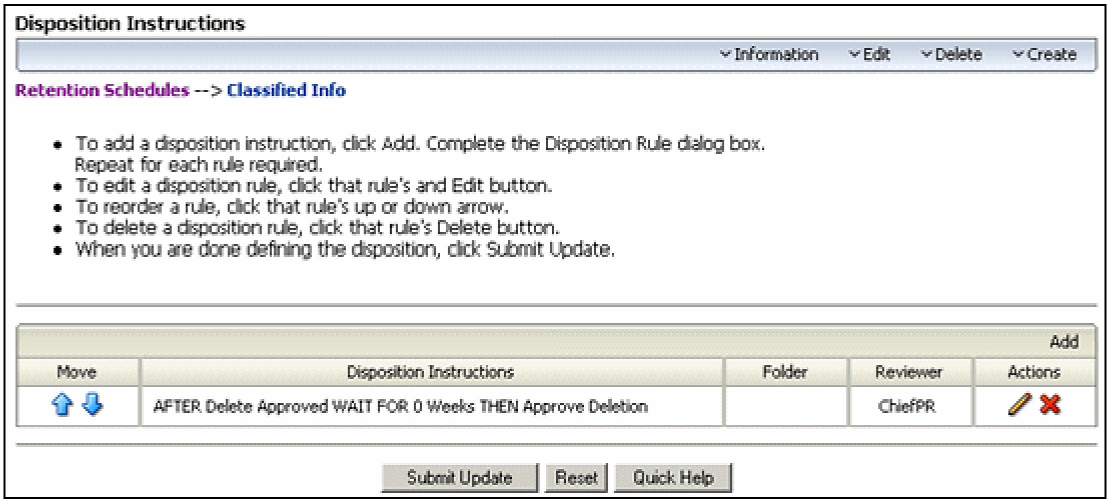
4. Define the first phase of the disposition, which is cut off at the end of the calendar year, retain in the current file area for one year, and then move to offline storage:
   a. In the **Triggering Event** list, select the **Retention Period Cutoff** option. The Retention Period field becomes available.
   b. In the **Retention Period** fields, enter `1` in the text box and select the **Calendar Years** period unit from the Retention Period list.
   c. In the **Disposition Action** list, select the **Move** option to move the records to offline storage.
   d. In the **Destination Location** box, type `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` in the text box and select the **Calendar Years** period unit from the Retention Period list.
   d. In the **Disposition Action** list, select the **Transfer** option to move the records 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 records 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** fields, enter `10` in the text box and select the **Calendar Years** period unit 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**. The successfully updated dispositions message is displayed.
8. Click **OK**.

DISPOSITION INTERFACE SCREENS

The following screens are used to manage dispositions:

- Disposition Instructions Page (page 14-24)
- Disposition Rule Screen (page 14-25)
- Disposition Information Page (page 14-28)

Disposition Instructions Page



Disposition Instructions

Retention Schedules --> Classified Info

- To add a disposition instruction, click Add. Complete the Disposition Rule dialog box. Repeat for each rule required.
- To edit a disposition rule, click that rule's and Edit button.
- To reorder a rule, click that rule's up or down arrow.
- To delete a disposition rule, click that rule's Delete button.
- When you are done defining the disposition, click Submit Update.

Add

Move	Disposition Instructions	Folder	Reviewer	Actions
⬆ ⬇	AFTER Delete Approved WAIT FOR 0 Weeks THEN Approve Deletion		ChiefPR	✎ ✖

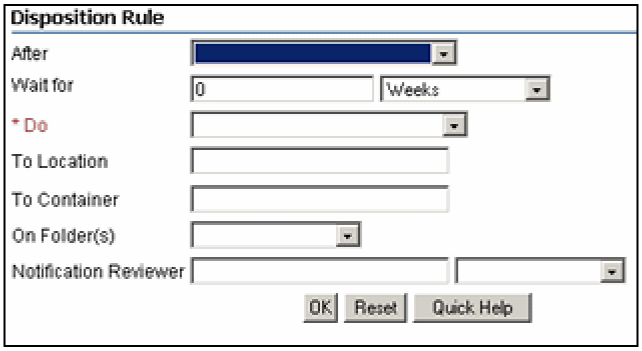
Use the Disposition Instructions page to add, edit, and delete disposition instructions for a retention category. To access it, browse content at the series level for the retention category. In the row for the retention category, click **Edit—Disposition Information** from the item **Actions** popup menu.

This page is displayed when you initially create a retention category. At the top of the page, there are bulleted instructions to assist you with its basic use.

Feature	Description
Disposition instructions box	Displays any defined disposition instructions for the retention category.
Up arrow (⬆) and Down arrow ⬇	Moves a selected disposition rule upward or downward one row with each click.

Feature	Description
Add button	Opens the Disposition Rule Screen (page 14-25), where you can define a new disposition rule.
Edit icon (✎)	Opens the Disposition Rule Screen (page 14-25) for the disposition rule selected within the Disposition Instructions box.
Delete (✖) button	Deletes the disposition rule selected within the Disposition Instructions box.
Submit Update button	Submits your updates.
Reset button	Resets the page to the initial default settings. If you are on an editing page, reset returns your original settings.

Disposition Rule Screen



Disposition Rule

After

Wait for 0 Weeks

* Do

To Location

To Container

On Folder(s)

Notification Reviewer

Use the Disposition Rule screen to define disposition rules for a retention category. To access it, browse content at the series level for the retention category. In the row for the retention category, click **Disposition Information** from the Actions popup list. From the **Actions** menu, click **Edit**. Click **Add**.

Depending on the captions settings in the Configure Records Management Page (page 7-2) page, there are two views of this screen: user-friendly captions for ease in reading disposition instructions, and standard captions for those organizations accustomed to disposition language. To view procedures for setting the captions, see Enabling or Disabling User-Friendly Captions (page 14-12).

Feature	Description
Triggering Event (user-friendly label = After)	Displays triggering events that you can associate with a disposition rule. See Triggering Events (page 14-5) for a list of available triggering events. ❖ Required.
Retention Period text box and list (user-friendly label = Wait for)	Enter the number of periods and select the period unit. The retention period represents how long to retain scheduled records and non-record content items. The list displays all periods defined, both built-in and custom. See Retention Periods (page 14-7) for a list of available retention period units. Required or optional depending on the disposition instruction scenario. For retention categories, you can specify a retention period only for the Retention Period Cutoff and Preceding Action triggering events. For non-record content item categories, you can specify a retention period for all triggering events. This enables you to create disposition rules for non-record content such as “Delete all old revisions three months after the last new revision was checked in.”
Disposition Action (user-friendly label = Do)	The disposition action defined for the rule. DoD Edition does not perform the action itself; rather, it sends an e-mail notification to the person responsible for carrying out the action. See Disposition Actions (page 14-8) for a list of available disposition actions. ❖ Required.
Destination Location (user-friendly label = To Location)	Specifies a physical location for an external folder; or a location for an accession, transfer, move, or archive disposition action. When you specify a location, the location information is added to the applicable records during action processing. ❖ Optional. ❖ Maximum characters: 30.

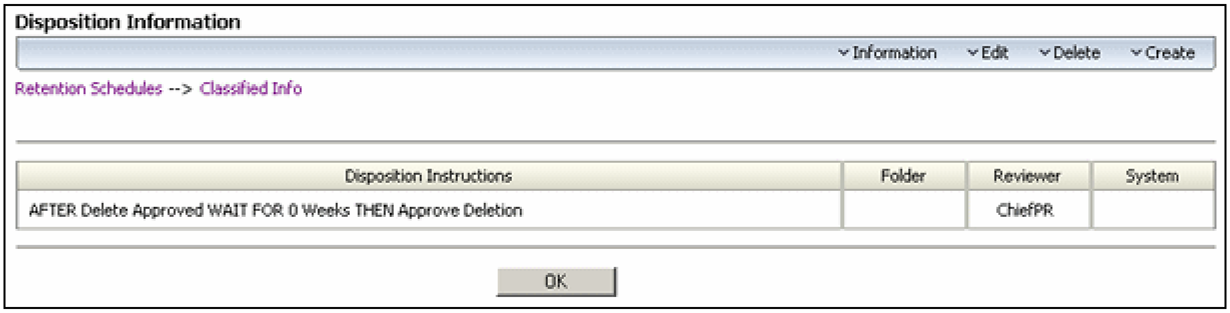
Feature	Description
Destination Container (user-friendly label = To Container)	Describes a physical container for an external records folder, such as a bar code or some other means of identification. ❖ Optional. ❖ Maximum characters: 30.
Apply to Records Folder list (user-friendly label = On Folder(s))	Applies a disposition rule to a specific records folder within a retention category. Any existing records folders within the retention category are displayed in the list. ❖ Optional. ❖ Default: All. The disposition rule is applied to all records folders within a retention category.
Notification Reviewer	This optional field allows you to specify who will be notified of the event. If you do not specify a user here, the category author will be notified. If you do specify an additional reviewer here, both the category author and the additional reviewer will be notified. You may also configure your system so that only the reviewer specified in this field is notified and not the category author (see Tech Tip below).
Reset button	Resets the page to the initial default settings. If you are editing a rule, reset returns your original settings.

Tech Tip: If you want the specified notification reviewer to be the only user that receives e-mail notifications for the events triggered by the disposition rule (and not the category author as well), make sure that the configuration file <*CS_Instance_Dir*>/custom/RecordsManagement/records_management_environment.cfg contains the following line:

```
RmaNotifyDispReviewerAndCatAuthor=false
```

You need to restart the content server for this setting to take effect.

Disposition Information Page



Disposition Information

Retention Schedules --> Classified Info

Disposition Instructions	Folder	Reviewer	System
AFTER Delete Approved WAIT FOR 0 Weeks THEN Approve Deletion		ChiefPR	

Use this page to view information about disposition instructions for a retention category. The records administrator can configure the disposition rules to display standard or user-friendly captions by toggling the captions setting on the Configure Records Management Page (page 7-2) page.

Permissions: Anyone with the Category.Read rights can view information disposition information for a retention category. All three predefined records management roles (‘rma’, ‘rmaprivileged’, and ‘rmaadmin’) have this role by default. To edit or delete disposition rules, the Category.Edit or Category.Delete rights are required.

To view this page, open the **Browse Content** tray, and click the **Retention Schedules** link. The Exploring Series “Retention Schedule” page is displayed. Navigate to the appropriate retention category.

Select **Information—Disposition Information** from the item’s **Actions** menu. You can also Info icon for the category and select **Information—Disposition Information** from the Page menu on the Retention Category Information Page (page 8-48).

Chapter

15

USING PROFILES

OVERVIEW

Records Management contains Simple Profiles functionality, which allows you to set up customized check-in, search, and updating pages based on your site's needs. Simple Profiles is fully documented in the document set available with the component. This chapter provides an overview of the functionality and how it interacts with the Records Management product. It disccusses the following topics:

- ❖ Managing Profiles (page 15-1)
- ❖ Records Management Profile Interface (page 15-2)

MANAGING PROFILES

Content profiles are used to configure the Check In, Update, Content Information, and Search pages. They limit or re-arrange the information displayed on these pages, thus making it easier for end users to see or enter only information which is directly relevant. Profiles can be considered a type of filter for what information will be displayed.

Follow this procedure to begin the profile creation process:

1. Select **Configure—Profiles** then the profile type from the Configure Records Management Page (page 7-2). If profiles already exist, choose Create Profile from the Page menu of the Profile Listing Page (page 15-2).

   The Profile Configuration Page (page 15-3) is displayed.

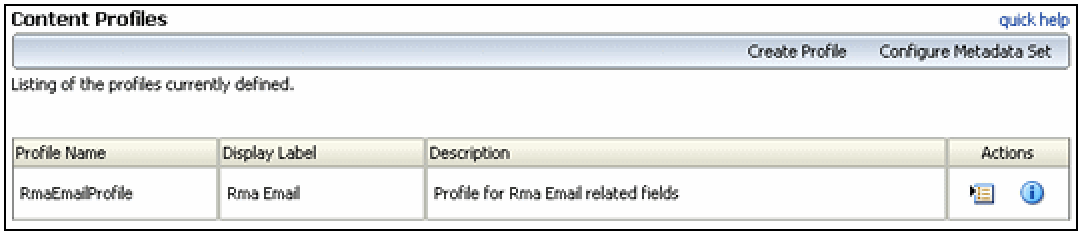
2. Select a trigger from the dropdown menu to use for the profiles for that type. This list is dependent on the type of trigger you chose to create (Content, Record Folder, or Retention Category).
3. Click **Save** when done or **Reset** to clear your choice and make a new selection.
4. A message is displayed, indicating the configuration was saved. Click **OK**.
5. The Profile Listing Page (page 15-2) is displayed. You can now create a new profile using that trigger.

Records Management Profile Interface

See the Simple Profiles documentation set for complete details about creating and using profiles.The following screens are specific to the Records Management product when using profiles:

- Profile Listing Page (page 15-2)
- Profile Configuration Page (page 15-3)

Profile Listing Page



Content Profiles

Listing of the profiles currently defined.

Profile Name	Display Label	Description	Actions
RmaEmailProfile	Rma Email	Profile for Rma Email related fields	☰ ⓘ

This page lists all available profiles. To access this page, select **Configure—Profiles** from the Configure Records Management Page (page 7-2).

The Page menu contains the following options:

- **Create Profile:** opens the initial screen used to create a profile of a specific type.
- **Configure Metadata Set**: lets you choose to change the metadata set used as a trigger for the profile type chosen.

The following options appear on the **Actions** menu for individual profiles:

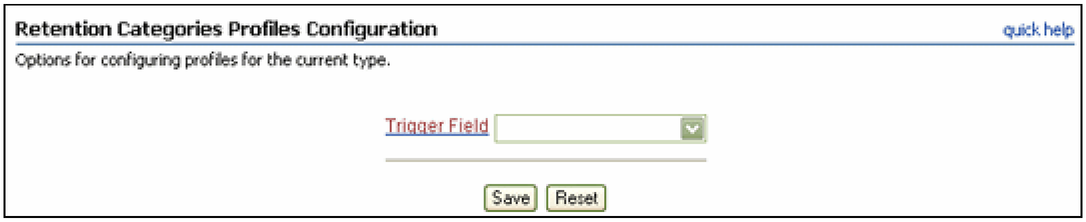
Profile Information: Displays an information page with details about the profiles.

Edit: Contains options allowing you to copy the profile, update it, or move it to the Configuration Manager, where it can be edited using the Content Server profile functionality.

Delete Profile: lets you delete any custom profiles.

Configure Profile and Configure Fields: accesses Simple Profile screens where you can change specific details in the profile, such as the labels, descriptions, field configurations, and the search order of fields.

Profile Configuration Page



Retention Categories Profiles Configuration

Options for configuring profiles for the current type.

This page is used to select a trigger for profiles of this type (content, records folder, or retention category).

This screen can be accessed in two way:

- If no triggers exist for content, records folders, or retention categories, this screen is displayed when you select **Configure—Profiles** and a profile type from the Configure Records Management Page (page 7-2).
- If triggers already exist and you wish to change the metadata set used for the profile, select **Configure Metadata Set** from the Profile Listing Page (page 15-2).

Appendix

A

THIRD PARTY LICENSES

OVERVIEW

This appendix includes a description of the Third Party Licenses for all the third party products included with this product.

- ❖ Apache Software License (page A-1)
- ❖ W3C® Software Notice and License (page A-2)
- ❖ Zlib License (page A-4)
- ❖ General BSD License (page A-5)
- ❖ General MIT License (page A-5)
- ❖ Unicode License (page A-6)
- ❖ Miscellaneous Attributions (page A-7)

APACHE SOFTWARE LICENSE

```
* Copyright 1999-2004 The Apache Software Foundation.

* Licensed under the Apache License, Version 2.0 (the "License");

* you may not use this file except in compliance with the License.

* You may obtain a copy of the License at

*      http://www.apache.org/licenses/LICENSE-2.0

*
```

```
* Unless required by applicable law or agreed to in writing, software
* distributed under the License is distributed on an "AS IS" BASIS,
 * WITHOUT WARRANTIES OR CONDITIONS OF ANY KIND, either express or implied.
 * See the License for the specific language governing permissions and
 * limitations under the License.
```

W3C® SOFTWARE NOTICE AND LICENSE

```
* Copyright © 1994-2000 World Wide Web Consortium,
* (Massachusetts Institute of Technology, Institut National de
* Recherche en Informatique et en Automatique, Keio University).
* All Rights Reserved.  http://www.w3.org/Consortium/Legal/
*
* This W3C work (including software, documents, or other related items) is
* being provided by the copyright holders under the following license. By
* obtaining, using and/or copying this work, you (the licensee) agree that
* you have read, understood, and will comply with the following terms and
* conditions:
*
* Permission to use, copy, modify, and distribute this software and its
* documentation, with or without modification, for any purpose and without
* fee or royalty is hereby granted, provided that you include the following
* on ALL copies of the software and documentation or portions thereof,
* including modifications, that you make:
*
*   1. The full text of this NOTICE in a location viewable to users of the
*      redistributed or derivative work.
*
*   2. Any pre-existing intellectual property disclaimers, notices, or terms
*      and conditions. If none exist, a short notice of the following form
*      (hypertext is preferred, text is permitted) should be used within the
*      body of any redistributed or derivative code: "Copyright ©
*      [$date-of-software] World Wide Web Consortium, (Massachusetts
*      Institute of Technology, Institut National de Recherche en
*      Informatique et en Automatique, Keio University). All Rights
*      Reserved. http://www.w3.org/Consortium/Legal/"
*
*   3. Notice of any changes or modifications to the W3C files, including the
*      date changes were made. (We recommend you provide URIs to the location
*      from which the code is derived.)
*
* THIS SOFTWARE AND DOCUMENTATION IS PROVIDED "AS IS," AND COPYRIGHT HOLDERS
* MAKE NO REPRESENTATIONS OR WARRANTIES, EXPRESS OR IMPLIED, INCLUDING BUT
* NOT LIMITED TO, WARRANTIES OF MERCHANTABILITY OR FITNESS FOR ANY PARTICULAR
* PURPOSE OR THAT THE USE OF THE SOFTWARE OR DOCUMENTATION WILL NOT INFRINGE
* ANY THIRD PARTY PATENTS, COPYRIGHTS, TRADEMARKS OR OTHER RIGHTS.
*
* COPYRIGHT HOLDERS WILL NOT BE LIABLE FOR ANY DIRECT, INDIRECT, SPECIAL OR
* CONSEQUENTIAL DAMAGES ARISING OUT OF ANY USE OF THE SOFTWARE OR
* DOCUMENTATION.
*
* The name and trademarks of copyright holders may NOT be used in advertising
* or publicity pertaining to the software without specific, written prior
* permission. Title to copyright in this software and any associated
* documentation will at all times remain with copyright holders.
*
```

ZLIB LICENSE

* zlib.h -- interface of the 'zlib' general purpose compression library
version 1.2.3, July 18th, 2005

Copyright (C) 1995-2005 Jean-loup Gailly and Mark Adler

This software is provided 'as-is', without any express or implied warranty. In no event will the authors be held liable for any damages arising from the use of this software.

Permission is granted to anyone to use this software for any purpose, including commercial applications, and to alter it and redistribute it freely, subject to the following restrictions:

1. The origin of this software must not be misrepresented; you must not claim that you wrote the original software. If you use this software in a product, an acknowledgment in the product documentation would be appreciated but is not required.
2. Altered source versions must be plainly marked as such, and must not be misrepresented as being the original software.
3. This notice may not be removed or altered from any source distribution.

Jean-loup Gailly jloup@gzip.org
Mark Adler madler@alumni.caltech.edu

GENERAL BSD LICENSE

Copyright (c) 1998, Regents of the University of California

All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

"Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.

"Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

"Neither the name of the <ORGANIZATION> nor the names of its contributors may be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDERS AND CONTRIBUTORS "AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE COPYRIGHT OWNER OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

GENERAL MIT LICENSE

Copyright (c) 1998, Regents of the Massachusetts Institute of Technology

Permission is hereby granted, free of charge, to any person obtaining a copy of this software and associated documentation files (the "Software"), to deal in the Software without restriction, including without limitation the rights to use, copy, modify, merge, publish, distribute, sublicense, and/or sell copies of the Software, and to permit persons to whom the Software is furnished to do so, subject to the following conditions:

The above copyright notice and this permission notice shall be included in all copies or substantial portions of the Software.

THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT. IN NO EVENT SHALL THE AUTHORS OR COPYRIGHT HOLDERS BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER LIABILITY, WHETHER IN AN ACTION OF CONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF OR IN CONNECTION WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS IN THE SOFTWARE.

UNICODE LICENSE

UNICODE, INC. LICENSE AGREEMENT - DATA FILES AND SOFTWARE

Unicode Data Files include all data files under the directories http://www.unicode.org/Public/, http://www.unicode.org/reports/, and http://www.unicode.org/cldr/data/ . Unicode Software includes any source code published in the Unicode Standard or under the directories http://www.unicode.org/Public/, http://www.unicode.org/reports/, and http://www.unicode.org/cldr/data/.

NOTICE TO USER: Carefully read the following legal agreement. BY DOWNLOADING, INSTALLING, COPYING OR OTHERWISE USING UNICODE INC.'S DATA FILES ("DATA FILES"), AND/OR SOFTWARE ("SOFTWARE"), YOU UNEQUIVOCALLY ACCEPT, AND AGREE TO BE BOUND BY, ALL OF THE TERMS AND CONDITIONS OF THIS AGREEMENT. IF YOU DO NOT AGREE, DO NOT DOWNLOAD, INSTALL, COPY, DISTRIBUTE OR USE THE DATA FILES OR SOFTWARE.

COPYRIGHT AND PERMISSION NOTICE

Copyright © 1991-2006 Unicode, Inc. All rights reserved. Distributed under the Terms of Use in http://www.unicode.org/copyright.html.

Permission is hereby granted, free of charge, to any person obtaining a copy of the Unicode data files and any associated documentation (the "Data Files") or Unicode software and any associated documentation (the "Software") to deal in the Data Files or Software without restriction, including without limitation the rights to use, copy, modify, merge, publish, distribute, and/or sell copies of the Data Files or Software, and to permit persons to whom the Data Files or Software are furnished to do so, provided that (a) the above copyright notice(s) and this permission notice appear with all copies of the Data Files or Software, (b) both the above copyright notice(s) and this permission notice appear in associated documentation, and (c) there is clear notice in each modified Data File or in the Software as well as in

MISCELLANEOUS ATTRIBUTIONS

Adobe, Acrobat, and the Acrobat Logo are registered trademarks of Adobe Systems Incorporated.

FAST Instream is a trademark of Fast Search and Transfer ASA.

HP-UX is a registered trademark of Hewlett-Packard Company.

IBM, Informix, and DB2 are registered trademarks of IBM Corporation.

Jaws PDF Library is a registered trademark of Global Graphics Software Ltd.

Kofax is a registered trademark, and Ascent and Ascent Capture are trademarks of Kofax Image Products.

Linux is a registered trademark of Linus Torvalds.

Mac is a registered trademark, and Safari is a trademark of Apple Computer, Inc.

Microsoft, Windows, and Internet Explorer are registered trademarks of Microsoft Corporation.

MrSID is property of LizardTech, Inc. It is protected by U.S. Patent No. 5,710,835. Foreign Patents Pending.

Oracle is a registered trademark of Oracle Corporation.

Portions Copyright © 1994-1997 LEAD Technologies, Inc. All rights reserved.

Glossary

G

GLOSSARY

accession

The transfer of legal and physical custody of permanent records to the National Archives.

audit trail

An electronic means of tracking interactions with records or non-record content items in a system so that any access to the record or content item within the system can be documented as it occurs or afterward. An audit trail may be used to identify unauthorized actions in relation to the items (for example, modification, deletion, or addition).

category

A description of a particular set of records or non-record content items within a retention schedule. Each category has retention and disposition data associated with it, applied to all records folders, non-record content items, and records within the category.

classified record

A record that requires protection against unauthorized disclosure (for example, because it contains information sensitive to the national security of the United States).
See also: unclassified record, declassified record.

classification guide

A mechanism that defines default values for a number of classification-related metadata fields on the content check-in page for records. This enables convenient implementation of multiple classification schemes in Records Manager DoD Edition.

classification markings

Identifications or markings that leave no doubt about the classified status of the information, the level of protection required, and the duration of the classification.

create

To file a new electronic record or content item and its associated metadata.

current record

Active record or content item. An record or content item record necessary to conduct current business, and therefore is generally maintained in an office space.
See also: noncurrent record or content item, semi-current record, permanent record.

custom disposition action

A disposition action defined by records administrators, as opposed to a disposition action that is built into Records Manager DoD Edition.
See also: disposition action.

custom period

A period defined by records administrators, as opposed to a period that is built into Records Manager DoD Edition.
See also: period.

custom security fields

Optional layer of security in addition to supplemental markings. As with supplemental markings, users must match the metadata field value to be allowed access to records. However, custom security fields allow you to configure *any* custom field (except date fields) that should be matched by a user rather than a designated supplemental marking. Also, custom security fields are enforced only at the record level whereas supplemental markings can be set at the record or record folder level.

custom supplemental markings

See: custom security fields.

custom trigger

A trigger defined by records administrators, as opposed to a trigger that is built into Records Manager DoD Edition.
See also: trigger.

cutoff

The moment that the status of a record or content item changes and the record or content item goes into disposition. A record or content item may be cut off after a specific period of time, at a specific event, or after a period of time after an event. Record or content items need to be cut off before they can be processed further in accordance with their disposition rules—for example, destroyed, transferred to an external storage facility, etc.

cycle

The periodic replacement of obsolete copies of content that is subject to review with copies of current content that is subject to review. This may occur daily, weekly, quarterly, annually, or at other designated intervals as specified by regulations or by the records administrator.

declassified record

A record that was formerly classified, but whose classified status has been lifted.
See also: classified record, unclassified record.

declassification

The authorized change in the status of information from classified to unclassified.
See also: downgrade, regrade, upgrade.

disposition

All actions to be taken when a retention period of a record or content item has ended and it has reached a designated disposition date.

disposition action

An individual operation to be performed when a retention period of a record or content item has ended and it has reached a designated disposition date.

disposition authority

Legal authority that empowers a United States Government agency to dispose of temporary records, or to transfer permanent records to the National Archives.
The disposition authority for permanent records must be obtained from NARA.
For certain temporary records, the authority must also be obtained from the General Accounting Office (GAO).

disposition instruction

A set of individual actions that are to be performed when a retention period of a record or non-record content item has ended and it has reached a designated disposition date.

downgrade

Determination by a declassification authority that information classified at a specified level shall be classified and safeguarded at a lower classification level.
See also: declassification, regrade, upgrade.

electronic record

A record stored in a form that a computer can process. Electronic items are also referred to as machine-readable records or content items.

essential record

See: subject to review.

event disposition

A disposition instruction in which a record is eligible for the specified disposition (transfer or destroy) upon or immediately after the specified event occurs. No retention period is applied.
See also: time disposition, time-event disposition.

external record

A non-record content item, physical or electronic, whose source file is not specifically stored in Records Manager DoD Edition. Records Manager DoD Edition can be used to track and search metadata associated with the external file, including disposition schedules, and can even manage an electronic rendition of an external file. An electronic rendition can be checked in as a primary file of an external record or content item, or be filed as a separate file, and then linked to the external file metadata.
See also: internal record.

file plan

See: retention schedule.

folder

A collection of similar records in the retention schedule. This allows records to be organized into groups. Records folders can be nested within other records folders.

FRC

Federal Records Center. A facility operated by NARA for low-cost storage and servicing of Federal records that are pending disposal or transfer to the National Archives.

freeze

To pause disposition processing of a record or content item, or record folder due to special circumstances, such as a lawsuit, court order, or investigation. Freezing record or content items temporarily extends an approved retention period.

inactive record

See noncurrent record or content item.

internal record

An electronic record stored within Records Manager DoD Edition.
See also: external record.

link

A defined relationship between record or content items. This may be useful when record or content items are related and need to be processed together.

media type

The material or environment on which the information of a record or content item is inscribed (for example, microform, electronic, paper).

metadata

Data describing stored data; that is, data describing the structure, data elements, interrelationships, and other characteristics of electronic records or content items.

move

To transfer records or content items and metadata out of the records management system.
See also: accession, transfer.

NARA

National Archives and Records Administration. Records repository for permanent records continually preserved by the Federal Government. The Archivist of the United States determines the historical or other value of records and deems the records as permanent.
See also: FRC.

noncurrent record or content item

Items no longer required to conduct business and therefore ready for final disposition.
See also: current record, semi-current record, permanent record.

non-record

A content item in Content Server that is not designated as a record (i.e., the ‘Is Record’ metadata field is not enabled).

original classification

An initial determination that information requires protection against unauthorized disclosure (for example, in the interest of national security).

originating organization

Official name or code identifying the office responsible for the creation of a document.

period

The segment of time that must pass before a review or disposition action can be performed. Records Manager DoD Edition comes with a number of built-in periods (for example, “one year”), but you also can create custom periods to meet your unique business needs.

permanent record

Records appraised by NARA as having sufficient historical or other value to warrant continued preservation by the Federal Government beyond the time they are normally needed for administrative, legal, or fiscal purposes. Records that are not authorized for destroying are retained permanently.

privileged user

An individual who is given special permission to perform functions beyond those of typical users.

publication date

The date and time that the author or originator completed the development of, or signed the document. For electronic documents, this date and time should be established by the author or from the time attribute assigned to the document by the application used to create the document. This is not necessarily the date or time that the document was filed in the records management system and thus became a record.

record

Any content item whose disposition and location must be tracked and maintained according to an organization’s requirements. Records include all books, papers, maps, photographs, machine-readable materials, or other documentary materials, regardless of physical form or characteristics.

record folder

See: folder.

retention schedule

The collective set of the series, categories, folders, and record or content item contained in a hierarchical structure.
See also: category.

records management

The planning, controlling, directing, organizing, training, promoting, and other managerial activities involving the life cycle of information, including creating, maintenance (use, storage, retrieval), and disposal, regardless of media.

records manager

An individual who is responsible for records management administration.

regrade

A determination by a classification or declassification authority that information classified and safeguarded at a specified level requires a different level of classification and safeguarding.
See also: declassification, downgrade, upgrade.

rendition

Replication of a content item that provides the same content but differs from the reference because of storage format or storage medium (for example, an HTML version generated from an original Word document).

rescind

To made void by an enacting authority.

retention period

Length of time that a record or content item must be kept in its repository before the record or content item can enter its final disposition instruction, such as destroy or archive.

screening

The process of aggregating and reviewing records or content items for management, review, and disposition purposes.

semi-current record

A record so seldom required that it should be moved to a holding area or to a records center.
See also: current record, noncurrent record or content item, permanent record.

series

A collection of retention categories in the retention schedule. You cannot file records or content items directly into a series; you must file the items into a category or record folder.

subject to review

Essential agency or private-sector business record or content items required to meet operational responsibilities in the event of a national security emergency or other emergency or disaster. Records subject to review also protect the legal and financial rights of the Government, businesses in the private sector, and individuals affected by the actions of Government and business. These record or content items are subject to periodic review and update. Also referred to as "essential records."

supersede

To supplant, or displace, an item by another item that is more recent or improved (superior).

supplemental markings

Record document markings not related to classification markings per se, but which elaborate or clarify document handling. Supplemental markings can be set at the record or record folder level, and can be used to restrict user access to records or records folders.
See also: custom supplemental markings.

temporary record

Records approved by NARA for disposal, immediately or after a retention period. Also referred to as "disposable records."

time disposition

A disposition instruction specifying when a record or content item is cut off, after which a fixed retention period is applied before disposition.
See also: event disposition, time-event disposition.

time-event disposition

A disposition instruction specifying that a record or content item is disposed of a fixed period of time after a predictable or specified event. After the specified event has

occurred, then the retention period is applied.
See also: event disposition, time disposition.

transfer

The process of moving records from one location to another; particularly, from an office space in which the record is used to storage facilities for temporary or permanent preservation. The legal and physical custody of transferred records is not affected (as opposed to accession).
See also: accession, move.

trigger

An event that needs to take place before a disposition instruction is processed. They are associated with disposition rules for retention categories. Examples of triggering events include changes in record state, completed processing of a preceding disposition action, and retention period cutoff.

unclassified record

A record that is not and has never been classified.
See also: classified record, declassified record.

upgrade

Determination by a declassification authority that information classified at a specified level shall be classified and safeguarded at a higher classification level.
See also: declassification, downgrade, regrade.

Index

I