Content Server Administration Tutorials
10*g* Release 3 (10.1.3.3.0)

March 2007

ORACLE

Content Server Administration Tutorials, 10*g* Release 3 (10.1.3.3.0)

Copyright © 2007, Oracle. All rights reserved.

Contributing Authors: Bruce Silver

Chapter 1: Understanding these Tutorials

Chapter 2: User Basics

Chapter 5: Library Folders

Chapter 6: Content Profiles

Chapter 7: The Repository Manager

Chapter 8: Workflows

UNDERSTANDING THESE TUTORIALS

OVERVIEW

These tutorials are designed to run in tandem with a Content Server instance in a non-production environment. They should not be used with Content Server instances that are functioning within an enterprise.

This section covers these topics:

❖ About These Tutorials (page 1-1)

❖ About Content Server (page 1-6)

❖ Before You Begin (page 1-4)

❖ Tutorial Scenario (page 1-8)

ABOUT THESE TUTORIALS

This section covers these topics:

❖ Intended Audience (page 1-2)

❖ Objectives (page 1-2)

❖ Duration (page 1-3)

❖ Conventions (page 1-3)

Intended Audience

These tutorials are for people who need to administer Content Server. They include administrators and sub-administrators:

❖ **Administrators** set up, maintain, and modify the configuration of the content management system and its user logins. To safeguard the integrity of the system, administrators require a user name and password to access the system. Common tasks for an administrator include configuring the system to manage and index files, archiving and replicating information, working with content server security, adjusting system properties, reviewing log files, etc.

❖ Enterprise administrators can set up sub-level administrators to perform a subset of administrative tasks within applications, specific departments, or security groups. These **sub-administrators** maintain a portion of a management system and its user logins.

The majority of administrators are sub-administrators. They administer portions of the software that correspond to the rights that the system administrator assigns to them.

Objectives

These tutorials introduce you to the basics of Content Server and take you through common administrative tasks step by step. In these tutorials you will perform the following tasks:

❖ Log in

❖ Change your user profile

❖ Check in new content

❖ Check out existing content

❖ Revise existing content

❖ Search for content

❖ Design a security model

❖ Build a hierarchy for your website

❖ Create active and historical reports

❖ Manage content, subscriptions, and indexing

❖ Create a workflow

Duration

There are seven tutorials in the series:

1. User Basics (see Chapter 2)

2. Security (see Chapter 3)

3. Accounts (see Chapter 4)

4. Library Folders (see Chapter 5)

5. Content Profiles (see Chapter 6)

6. The Repository Manager (see Chapter 7)

7. Workflows (see Chapter 8)

Each tutorial takes between 30 and 60 minutes to complete. The entire series of tutorials should take three to five hours. You can pause between tutorials, but you should complete each tutorial in the order presented before moving on to the next.

Conventions

The following symbols are used throughout this tutorial:

Symbols	Description
	This is a **note** symbol. It is used to bring special attention to information.
	This is a **technical tip** symbol. It is used to identify information that can be used to make your tasks easier.
	This is an **important** notice symbol. It is used to identify a required step or required information.
	This is a **caution** symbol. It is used to identify information that might cause loss of data or serious system problems.

BEFORE YOU BEGIN

This section covers these topics:

❖ Setup (page 1-4)

❖ Browser Configuration (page 1-5)

Setup

Before you begin these tutorials, make sure that a Content Server instance and the tutorial files are available.

1. Make sure that the Content Server software is installed in a non-production environment.

Caution: These tutorials should be used in a development environment *only.* They should *not* be used with Content Server instances that are functioning within an enterprise.

2. The *Ruggans Tutorial Files* folder is located in the *documentation/samples/tutorial* directory on the Content Server software distribution CD labeled 'Documentation'. Open the *Ruggans Tutorial Files* folder and verify that the following files are located in the folder:

    documentation\samples\tutorial\Ruggans Tutorial Files\
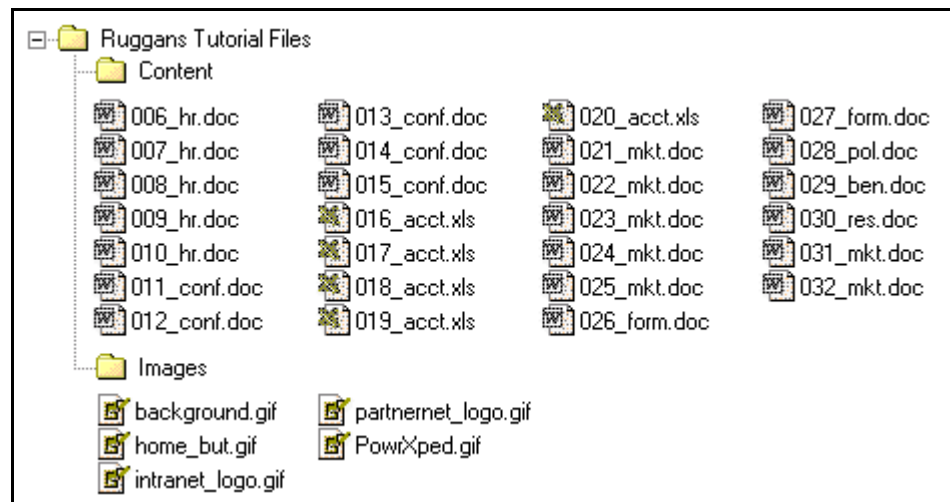
Browser Configuration

For Content Server to run efficiently, set your browser options to check for new content each time you visit a page.

Configuring Browser Options

For Internet Explorer:

1. Select **Tools—Internet Options**. The *Internet Options* screen is displayed.

2. Click **Settings**. The *Settings* screen is displayed.

3. Enable **Every visit to the page** and click **OK**. The *Settings* screen closes.

4. Click **OK** again to close the *Internet Options* screen.

5. Restart Internet Explorer.

For Firefox:

1. Enter **about:config** into the address bar. A list of configuration entries is displayed.

2. Enter **browser.cache** in the **Filter** field. A list of browser configuration entries is displayed.

3. Double-click **browser.cache.check_doc_frequency**. The *Enter Integer value* screen is displayed.

4. Change the setting to **1** and click **OK**.

5. Restart Firefox.

For Safari on a Macintosh:

No default cache settings are available in Safari on a Macintosh computer. To empty the cache in Safari, select **Safari—Empty Cache**.

ABOUT CONTENT SERVER

This section covers these topics:

❖

❖

System Purpose

Content Server is an automated system for sharing, managing, and distributing business information to partners, suppliers, and customers using a Web site. The software was built to enable rapid deployment of unstructured information—documents, HTML pages, images, audio and video clips, policies and procedures, engineering specifications, and so forth—that is typically unmanaged. Designed for the Web, it is considered the unrivaled solution for building secure business libraries with check in/check out, revision control, and automated publishing in Web-ready formats. Content Server is:

Secure

You can secure content and authorize users through Security Groups, Roles, and Accounts.

Immediate

Current information is available to authorized users as soon as it is released.

Flexible

You can link any type of content—letters, reports, engineering drawings, spreadsheets, manuals, sales literature, and more—under one powerful system of knowledge distribution, and create fields for metadata unique to your organization. Through Component Architecture, you can even modify the look and feel to mimic your corporate web site. Refer to the manuals in the *documentation/developer* folder on Content Server CD labeled 'Documentation' for more information.

System Users

The software is designed for two types of users: those who need to find, view, and print content items—called **consumers—**and those who need to create and revise content items—called **contributors**.

The majority of the users are consumers. These users do not need a user name and password to get into the system unless security is placed on the content items. To safeguard the integrity of the content items, the contributors need a user name and password to check content items in and out of the system.

BEHIND THE SCENES

This section covers these topics:

❖ How Content Server Works (page 1-7)

❖ What Content Server Does (page 1-7)

❖ Tutorial Scenario (page 1-8)

How Content Server Works

Content Server is based on an open architecture. It uses standard browsers, like Firefox or Internet Explorer, across multiple platforms, and communicates through HTTP and CGI. Content Server can be installed on Windows, Sun, HP-UX, IBM AIX, and Linux platforms.

The software was written in Java, which means most of the administration tools are accessible on a local PC. This means you do not need to perform all administration tasks from the server.

What Content Server Does

In general, when a file is checked into the system, it is processed through a conversion tool, such as the PDF Converter or Dynamic Converter, resulting in a Web-viewable version of the file, such as PDF or HTML.

Original files are stored in a specified *vault* directory.

Web-viewable files are stored in a specified *weblayout* directory.

Before being released for viewing on the Web site, each file is processed through the Indexer. The Indexer indexes information about the file, called *content information* or *metadata*, and stores the metadata in an SQL database. For file formats that are supported by the search engine, the Indexer also indexes the full text of the file. The indexing process can then be repeated at specified intervals to update any changes to the metadata for content that has been released.

Content Server connects to the following databases:

❖ Microsoft SQL Server (2000 SP4, 2005)

❖ Oracle (9.2, 10g)

❖ Sybase (15)

❖ PostgreSQL (8.01)

❖ DB2 (8.1, 8.2)

If your index collection is growing too large or it is taking too long to index a large quantity of files, you can index just metadata and not every word in your files. For more information, see "Working with the Search Index" in Content Server Help.

Tutorial Scenario

For these tutorials, you are the system administrator of the Ruggans Financial Corporation. Your company has just purchased Content Server, and you have been assigned to set up the system to provide secure access to the appropriate people.

Let's become familiar with Content Server by performing some basic tasks required of a typical user.

USER BASICS

OVERVIEW

This section covers these topics:

It is recommended that you go through this tutorial from beginning to end, in the suggested order.

GETTING STARTED

As the system administrator for Ruggans Financial Corporation, you are responsible for checking content in to the Oracle content management system. First, you need to open a server instance in your browser and log in. To get started:

1. Open your web browser.

2. Type *http://<Your_Instance_Name>/<install_dir>/<instance_dir>/* in the address bar (for example, *http://Master_on_mjones/<install_dir>/<instance_dir>/*).

You can quickly access and search public content without logging in. In order to access content with full privileges, you must log in.

GETTING AROUND

Clicking the icons or text menu enables you to navigate within the Content Server.

Icon	Link	Description
	[Login]	Enables you to log in to Content Server.
	[Home]	Opens the main home page.
	[Library]	Opens a library page that you, as system administrator, will set up with links pertinent to your organization.
	[Search]	Opens a standard search page.

LOGGING IN

After you have logged in, you can access your user profile, the Content Manager, and any custom links that are set up from the *tray area* at the left side of the screen. During a browser session, you are authenticated the first time you log in to Content Server. You do not have to log in again unless you start a new browser session.

Logging into Content Server is required to perform the following functions:

❖ Viewing secure content

❖ Checking content into Content Server

❖ Accessing the administration screens

Note: Content Server logins can also be integrated with Microsoft network security models. See the *Managing Security and User Access* guide and online help for more information on using Content Server with Microsoft network security models.

To log in to Content Server, complete the following steps:

1. Click **Login**. The Enter Network Password screen is displayed.

2. Enter **sysadmin** in the **User Name** field.

3. Enter **idc** in the **Password** field.

Caution: The password **idc** is the default password assigned to the system administrator. It is strongly recommended that you change the system administrator password to help keep your system secure.

4. Click **OK**. The Home page is displayed.

CHANGING YOUR USER PROFILE

The User Profile page holds information about your name, password, email address, and view preferences. To review or update this information, complete the following steps:

1. In the main menu, click **My Profile**. The User Profile for 'sysadmin' is displayed.

2. Select the information in the **Full Name** field and enter your name.

3. In the User Personalization Settings area, select the **Email Format**, **Layout**, **Skin**, and **Search Template** options you prefer.

4. Click **Update**. Your selections take effect.

CONTENT MANAGEMENT
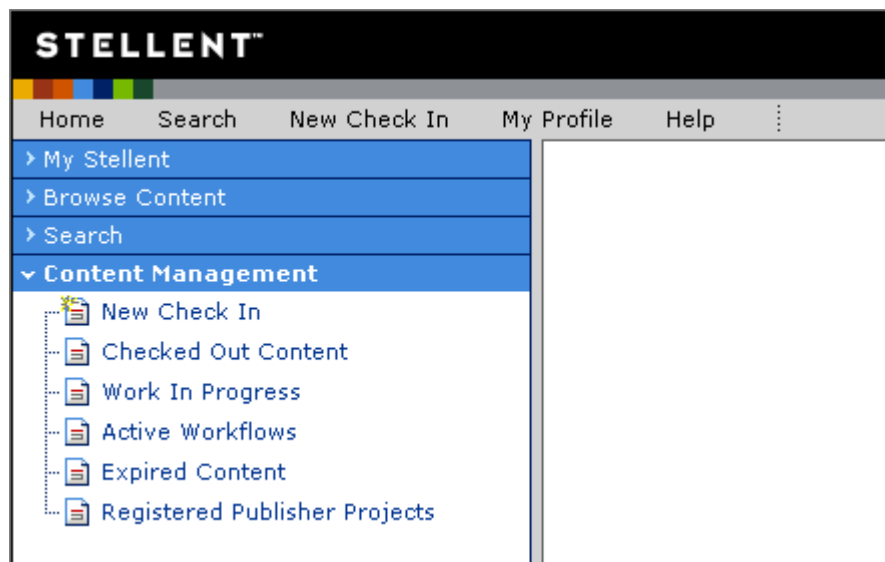
Files in their native format (that is, the format they were originally created in) are stored in a central repository from which you can check the files in and out. Only one person is allowed to have a file checked out at a time, but many people can view the released version of the file. Use the Content Management feature to check content in and out of the Content Server repository and to monitor the status of content.

To open Content Management:

1. In the portal, click **Content Management**. The Content Management tray is opened.

    The Content Management links are described in the following table:

Link	Description
New Check In	Links to the Content Check In page where you can check in new content.
Checked Out Content	Lists all the content to which you have permission that is currently checked out.
Work In Progress	Lists the content currently in the Content Server process that has not yet been released.

Link	Description
Active Workflows	Lists any active workflows and the content associated with each.
Expired Content	Opens the Content Expiration page, which enables you to search for expired or about to expire content.
Registered Publisher Projects	Lists any registered projects. This option is applicable only when Content Publisher, an optional add-on to Content Server, is installed.

2. Click **New Check In.** The Content Check In Form is displayed.

Figure 2-1 Example Content Check In Form

CHECKING IN NEW CONTENT - REQUIRED FIELDS

The Content Check In Form has a number of content information fields, also referred to as *metadata fields*. Metadata is essentially data about data. The content information fields provide information about the content, which enables the system to keep track of content and assists users when searching for content. There are a number of predefined fields, and you can also add custom fields to suit your specific applications. You can add required or optional custom metadata fields. All standard fields displayed in red are required fields. You must complete all required fields before you can check a file into the system.

CHECKING IN NEW CONTENT - OPTIONAL FIELDS

All fields on the Content Check In Form displayed in black are optional fields. You do not have to complete optional fields when you check a file is in to the system.
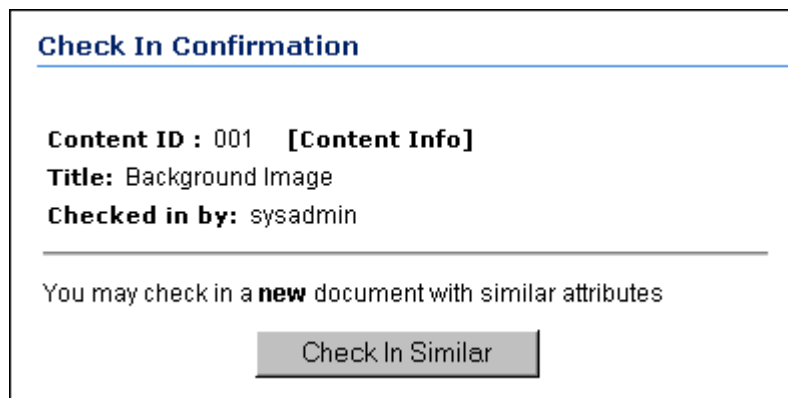
CHECKING IN A FILE

Use this tutorial to learn how to check in a file. To check in a file, complete the following steps:

1. On the Content Check In Form, type **001** in the **Content ID** field. Leave the **Type, Author,** and **Security Group** fields set to the default.

2. Next to the **Primary File** field, click **Browse**. The Choose File dialog box is displayed.

3. Find and select the **background.gif** file located in the *Ruggans Tutorial Files/Images* folder.

4. Click **Open**. The file name and path displays in the **Primary File** field on the Content Check In Form.

5. Type **Background Image** in the **Title** field.

6. Click **Check In**. The Check In Confirmation page is displayed to confirm that the content item was checked in successfully.

Figure 2-2   Example Check In Confirmation page

You can also use this form to check in a similar file. When you click **Check in Similar**, the Check In Content Form is displayed with some fields already populated for you.

CHECKING OUT A FILE

To revise a content item, you need to check it out and then check it back in when you have finished editing the content. Only one person at a time can check out a revision, but others can continue to view the released file.

To check out a file:

1. On the main menu, click the **Search** link. The Search page is displayed.

Figure 2-3   Example Search Page

2. Click **Search** to search for all content that has been checked in. The content item with content ID '001' is displayed on the search results page.

3. Click on the **Info** icon. The Content Information page is displayed.

Figure 2-4   Example Content Information Page with Check Out Action selected

4. From the **Actions** list, choose **Check Out**. The Check Out Confirmation page is displayed.

Figure 2-5   Example Check Out Confirmation page

Check Out Confirmation

Title: Background Image
Content ID : 001
Checked Out By: sysadmin

It is **strongly** recommended that you save the file to a directory other than the browser's default directory. Use the right mouse button on the link below to choose a save option.

Native File Link: background.gif

Click on the **Check In** button below when your edit is complete.

Check In

At this point, you can edit the file in its native application or you could choose to replace the file with a different one. You can keep the same file name, or use a different one. For this tutorial, you save a copy of the file to your hard drive with a different file name.

5. To get a copy of the original file, click the file name following **Native File Link**. The File Download dialog box is displayed. Click **Save**.

6. On the Save As screen, navigate to the location on your hard drive where you want to save the file.

7. Change the file name to **background_1.gif** and click **Save**.

8. You are now ready to check in the revised file. On the Check Out Confirmation page, click **Check In**. The Content Check In Form is displayed with the metadata fields. The Original File field shows the file name of the content item that was checked out.

Figure 2-6 Example Content Check In Form

9. Click **Browse** next to the **Primary File** field and navigate to the **background_1.gif** file.

10. Select the **background_1.gif** file and click **Open**.

11. Click **Check In**.

    The Check In Confirmation page is displayed.

12. Search for the 001 content item again. Note that the revision number is now 2 on the Content Information page.

EXERCISE 1: CHECKING IN CONTENT

For this exercise, all of the files located in the *Ruggans Tutorial Files/Images* folder need to be checked in.

Note: Only check in the files in the Images folder at this time. You will check in files in the Content folder in later exercises.

1. Verify that the Content Check In Form is displayed. If it is not, click **Content Manager** in the portal page, then click **New Check In**.

2. Starting with **002**, type the next sequential number into the **Content ID** field. (Remember **001** was used for **background.gif**, the first file you checked in.) Leave the **Type, Author,** and **Security Group** fields set to the default.

3. Click **Browse**, which is next to the **Primary File** field, and navigate to the *Ruggans Tutorial Files/Images* folder.

4. Select the file to check in.

5. Click **Open**.

6. Type the file name into the **Title** field.

7. Click **Check In**. The Check In Confirmation page is displayed to inform you that the content item was checked in successfully. Click **Check In Similar** to check in additional files with similar attributes.

8. Repeat steps 2 through 8 until all the files in the *Ruggans Tutorial Files/Images* folder are checked in.

You can now proceed with Tutorial 2: Security (see Chapter 3).

3

SECURITY

OVERVIEW

This section covers these topics:

It is recommended that you go through this tutorial from beginning to end, in the suggested order.

SECURITY OVERVIEW

Setting up a security model depends on your business structure and who needs access to what content. This can vary greatly from company to company. Therefore, we will discuss standard security models and guidelines for setting up security for your company.

Security is made up of the following four items:

Name	Description
Security Groups	Security Groups are groupings of content to which you control access through roles. They are not groups of people as they are in Windows 2000 or 2003.
Roles	Roles define the permissions (Read, Write, Delete, and Admin) that users have to specific security groups. Each user is assigned one or more roles.
Users	Users are the logins made up of a user name and password. Users are assigned one or more roles (and one or more accounts if accounts are enabled). You can also assign an alias to a group of users.
Accounts	Accounts can be activated to provide greater flexibility and granularity than security groups alone.

Content is secured through Content Server security with user names and passwords stored in Content Server. Users can view only the content for which they have read permission, whether the content is accessed through a search or through the Library.

USING EXTERNAL SECURITY

Content Server security can be internal, where user security is set up within Content Server using the User Admin application. This type of security is used in these tutorials. Content Server security can also be external, where Content Server is integrated with an external user base, such as NTLM, Active Directory, or other LDAP server. When users log in to the content server, they are assigned roles and accounts based on their user attributes defined in the external system.

User logins, passwords, and permissions can be derived from one of the following external user bases:

❖ **NTLM**—A user's Windows network credentials are used to authenticate the user in the content server.

Important: NTLM is not supported with Windows 2003. ADSI works well on Windows 2003 and is recommended for that platform.

❖ **Active Directory**—User information is stored in a Microsoft Active Directory user base.

❖ **LDAP**—User information is stored in an LDAP-compliant user base, such as iPlanet.

❖ **Active Directory with LDAP Provider**—User information is stored in a Microsoft Active Directory user base, which the content server accesses using an LDAP provider. This may be the preferred approach if your network includes the following:

• Content server access through non-Internet Explorer client browsers

• Content server installed on a UNIX operating system

• Firewall between the content server and user base computers

A custom Active Directory LDAP component is required for this type of security integration.

For this tutorial, security is set up using the internal method. For ore information on external security, refer to the *Managing Security and User Access Guide*.

THE SECURITY MODEL

This section covers these topics:

Users, Roles, and Security Groups

The relationship between users, roles, and security groups is depicted in the tutorial security model figure. Keep in mind that you can have one or more security groups and one or more roles in any combination. Accounts will be added to this model and described in the next tutorial.

Figure 3-7 Tutorial Security Model
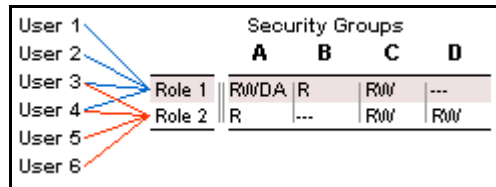
As content is checked into Content Server, it is assigned to a security group. As system administrator, you will assign each user to one or more roles. Each role defines the permissions a user has to the content in each security group.

Designing a Security Model

Planning is essential to a well designed, low maintenance, efficient security model. Gather information and develop a security model to fit your company requirements. Things to consider include:

❖ Who needs access to what?

❖ Do you need to use accounts?

❖ Are there any migrated data requirements?

SECURITY GROUPS

This section covers these topics:

❖ Overview (page 3-4)

❖ Creating Security Groups (page 3-5)

Overview

A security group is a set of content grouped under a unique name to which you want to control access. The following are general guidelines in defining security groups:

❖ Security group names have a maximum field length of 30 characters. The following characters are not allowed in the security group name: spaces, tabs, linefeeds, carriage returns, and the symbols ; : ^ ? : @ & + " # % < > * ~. The description for the security group has a maximum field length of 80 characters.

❖ Choose only static information as a security group. For example, department names change infrequently, so they can be considered static; projects come and go, so they might not be considered static.

❖ Organize security groups into logical, manageable groups of content.

Creating Security Groups

Content Server comes with two predefined security groups: **Public** and **Secure**.

As system administrator for the Ruggans Financial Corporation, you have spoken to the users and determined that for this initial implementation, you need to define three additional security groups: **HR**, **Accounting**, and **Confidential**. For this tutorial, you will define the HR group. The remaining groups you will add in the exercise at the end of this tutorial.

To create the HR security group, complete the following steps:

1. From the Administration tray, choose **Admin Applets**. The Administration page is displayed.

2. Click **User Admin**. The User Admin application is displayed.

Figure 3-8   User Admin Application
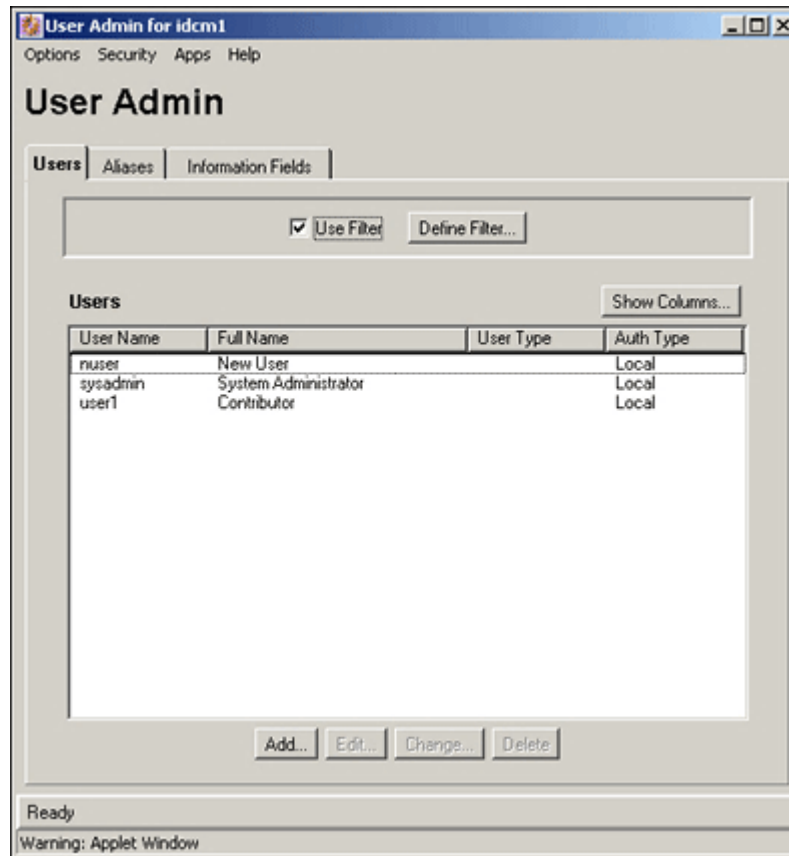
3.   Select **Security—Permissions by Group** from the User Admin menu bar. The
      Permissions by Group screen is displayed.

Figure 3-9   Permissions By Group Screen
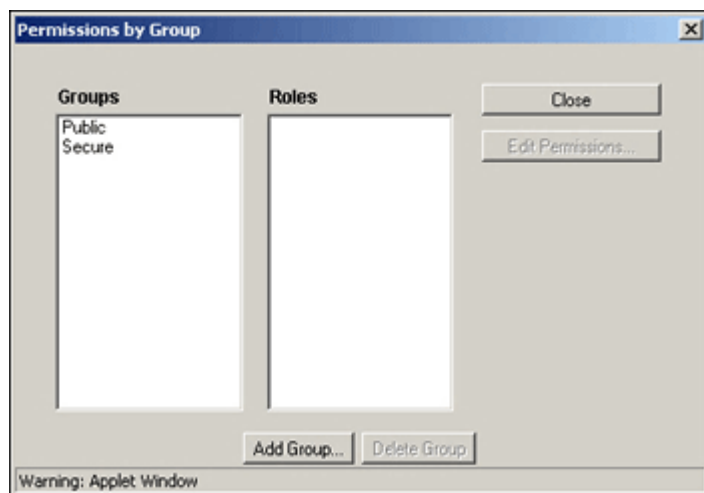
4. Click **Add Group**. The Add New Group screen is displayed.

5. Enter **HR** in the **Group Name** box and **HR Policies and Forms** in the **Description** box.

6. Click **OK**. The HR group displays in the Groups list of the Permissions by Group screen.

7. Click **Close** on the **Permissions By Group** screen.

8. Close the **User Admin** screen.

ROLES

This section covers these topics:

❖ Overview (page 3-8)

❖ Role Guidelines (page 3-8)

❖ Predefined Roles (page 3-9)

❖ Creating Roles (page 3-9)

❖ Assigning Roles (page 3-17)

Overview

Roles define the permissions a user has for each security group. Roles also define access rights to the tools necessary for a sub admin, who is a user who has been given some administrative rights.

For example, the role of HRAdmin may have Read, Write, and Delete permission to all content in the HR Security Group, but only Read permission to all Public content, and no permissions to other content.

Users can be assigned more than one role. If roles overlap, the permissions are added together.

Important: If roles overlap, the permissions are added together. For example, if role 1 has Read permission to a specific security group and role 2 has Read, Write and Delete permission to the same security group, a user with both roles has Read, Write and Delete permission to that security group.

Role Guidelines

Role names can have a maximum of 30 alphanumeric characters. Spaces and special characters are allowed.

Predefined Roles

Content Server comes with the following four predefined roles:

Role	Description
Guest	A user who has Read permission to the security group of Public. No login is required. Give this role to all guest and anonymous users.
Contributor	A user who has Read and Write permission to the security group of Public. Give this role to users who need to not only view, but also revise content in the Public security group.
Sysmanager	A user who has Read permission to the security groups of Public and Secure and permission to access the Admin Server, but not access to all the administration tools. Give this role to a user who needs access to start and stop the Content Admin Server.
Admin	A user who has Read, Write, Delete, and Admin permission to all security groups and access to all administration tools. Give this role to an administrator.

Creating Roles

To create a new role, complete the following steps:

1. Click **User Admin**. The User Admin application is displayed.

2. Select **Security—Permissions by Role** from the User Admin menu bar. The Permissions by Role screen is displayed.

Figure 3-10 Permissions by Role Screen
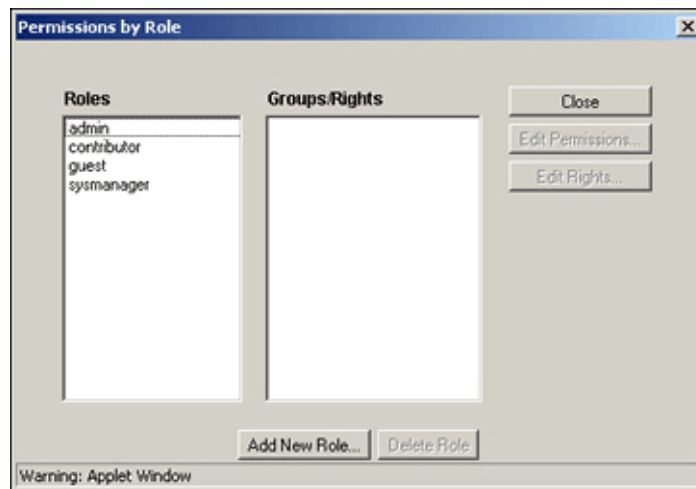
3. Click **Add New Role**. The Add New Role screen is displayed.

4. Enter **HRAdmin** for the Role Name.

Note: Role names have a maximum of 30 alphanumeric characters. Spaces and special characters are allowed.
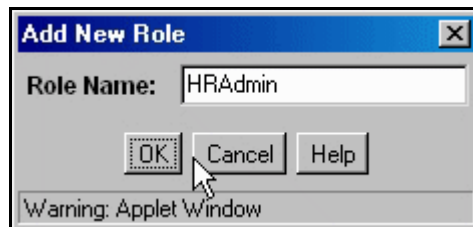
5. Click **OK**.

6. Select the new role **HRAdmin** in the **Roles** list. Permissions for the selected role are displayed in the **Groups/Rights** list.

7. Click **Close** to close the Permissions by Role screen.

8. Close the User Admin applet.

PERMISSIONS

There are four levels of permissions:

Level	Description
Read	Users may only search for, view, and print content.
Write	Users may check in, check out, and get a copy of content, but cannot delete content.
Delete	Users may delete content.
Admin	Users have rights to the system administration tools. Users may check in content that they did not author. (By default, only the author can check in content they checked out.) Users may change the Author field on the Content Check In Form page to a local user.

Note: Each level of permission includes the permissions at the lower levels. For example, a user with Delete permission also has Read and Write permission.

Assigning Permissions

You can assign or change permissions to any role at any time by doing the following steps.

1. Click **User Admin**. The User Admin screen is displayed.

2. Select **Security—Permissions by Role** from the User Admin menu bar. The Permissions by Role screen is displayed.

3. Select the **HRAdmin** role in the **Roles** list and the **HR** Security Group in the **Groups/Rights** list to edit the permissions for this role. **Edit Permissions** becomes available.

Note: Initially a role is assigned Read (R) permissions to the Public security group and no permissions to all the other defined security groups.

4. Click **Edit Permissions**. The Edit Permissions screen is displayed.

5. Enable the **Delete** check box for this role. Notice that **Read** and **Write** check boxes are selected automatically.

6. Click **OK**.

7. Click **Close** on the Permissions By Role screen.

RIGHTS

As roles and permissions allow users to access and administer content, rights allow users to access system administration tools. Rights are assigned to a role. Using rights, the system administrator can set up sub-administrators with roles that allow them to access one or more of the following administration applets:

❖ User Admin

❖ Web Layout Editor

❖ Repository Manager

❖ Workflow Admin

❖ Configuration Manager

❖ Archiver

Important: Not all functions of an administration applet are available to a user given sub-admin rights to that applet. Only the *sysadmin* user can change a user's rights.

Note: The use of each of these applets is described later in these tutorials, with the exception of the Archiver applet. See the *System Migration Guide* and online help for information on the Archiver applet.

Assigning Rights

To assign rights, complete the following steps:

1. Select **Security—Permissions by Role** from the User Admin menu bar. The Permissions by Role screen is displayed.

2. Select the **HRAdmin** role in the **Roles** list to edit the rights for this role.

3. Click **Edit Applet Rights**.

4. Select the **Rights.Apps.UserAdmin** and **Rights.Apps.Workflow** options for this role.

5. Click **OK**.

6. Click **Close** on the **Permissions By Role** screen.

USER GUIDELINES

New users of your system are also added using the User Admin screen on the Administration page. The User Name has a maximum field length of 30 alphanumeric characters and the Password has a maximum field length of 50 alphanumeric characters.

This section covers these topics:

❖ Predefined Users (page 3-13)

❖ Adding a New User (page 3-14)

❖ Adding a Custom User Information Field (page 3-15)

❖ Assigning Roles (page 3-17)

Predefined Users

Content Server comes with two predefined users:

Name	Description
user1	User1 has a default password of *"idc"* and belongs to the contributor role. Use the **user1** for testing purposes only and delete **user1** before going into production.
sysadmin	Sysadmin has a default password of *"idc"* and belongs to the admin role. It is used by the System Administrator. Do not delete the **sysadmin** user, but change the password before going into production.

Note: User names are case-sensitive.

Adding a New User

Use this tutorial to add a new user.

1. Click **Add** on the User Admin screen. The Choose the Authorization Type screen is displayed.

   The following Authorization Type options are available:

Type	Description
Local	Use the Local type when you have fewer than 500 users. Each local user is displayed in the **Author** choice list on the Content Check In Form.
Global	Use the Global type when you have more than 500 users. Because this makes the **Author** choice list too extensive, you can add additional user information to the Organization Path field, enabling you to filter the user listing based on the additional information. For example, if you categorize Ruggans users hierarchically, you could display a list of the Accounting department by location—Minneapolis, Seattle, and Boston—using Accounting/MSP, Accounting/SEA, and Accounting/BOS.
External	Use the External type when a login is from somewhere other than within Content Server. This can be from a Microsoft Network Login or another database, like LDAP. Note that External is not a choice in the Authorization Type choice list. It requires services to implement.

2. Select **Local** and click **OK**. The Add User screen is displayed.

3. Type **jdoe** in the **Name** field.

4. Type **Jane Doe** in the **Full Name** field.

5. Type **idc** in the **Password** field, and again in the **Confirm Password** field.

Note: Logins are case-sensitive.

6. Type **jane.doe@yourcompany.com** in the **E-Mail Address** field.

Note: The e-mail address must be filled in for subscriptions and workflows to work properly.

7. Click **OK**. The Add User screen closes, and the new user displays in the **Users** list.

Adding a Custom User Information Field

Use this tutorial to add a custom information field to user information.

To add a custom user information field:

1. In the User Admin screen, click the **Information Fields** tab. The Field Information for users is displayed.

Figure 3-11 Information Fields tab in the User Admin screen
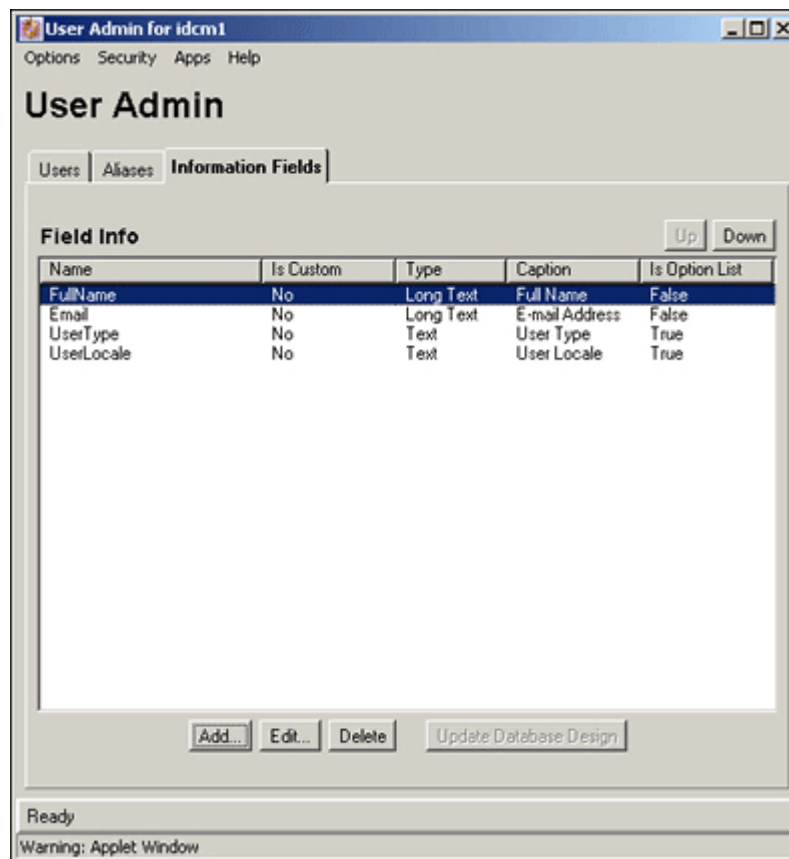
2. Click **Add**. The Add Custom Info Field screen is displayed.

3. Enter `CellPhone` in the **Field Name** box. Spaces are not allowed in the field name.

4. Click **OK**. The Add Custom Info Field '*fieldname*' screen is displayed so you can enter additional information about the field.
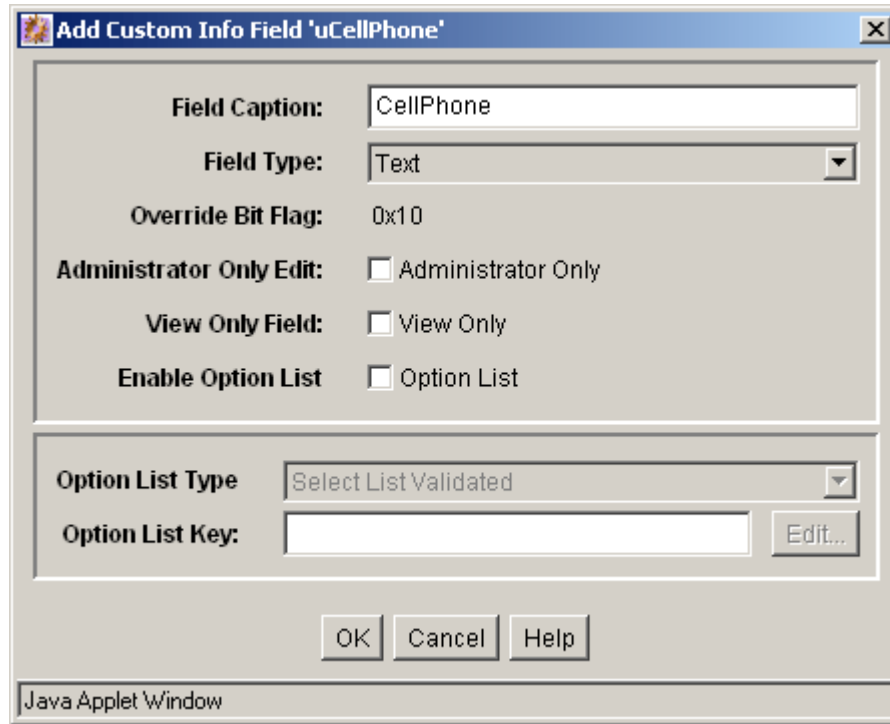
5. Enter a space between 'Cell' and 'Phone' in the **Field Caption** and click **OK**. The Update Database Design screen is displayed.
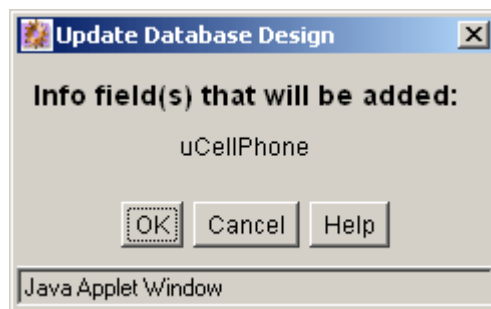
6. Click **OK**. The new field displays in the Field Info list in the Information Fields tab.

7. To display the new user field in the Users tab, click the **Users** tab, click **Show Columns**, and select the new Cell Phone field in the Show Columns screen.

Assigning Roles

Each user must be assigned at least one role. If a user is assigned more than one role, the permissions from each role are added together.

Note: A user must be assigned a role in order to access content. If a user is not assigned a role, the user cannot access any content.

1. In the User Admin screen, select **jdoe** in the **Users** list and click **Edit**. The Edit User screen is displayed.

2. Click the **Roles** tab.

3. In the Roles tab, click **Add Role**. The Add Role screen is displayed.

4. Select **HRAdmin** in the **Role Name** list.

5. Click **OK** to close the Add Role screen.

6. Click **OK** to close the Edit User screen.

ALIASES

An *alias* enables you to assign a user name to a job function or to a group of users so you do not have to specify them individually. Aliases are useful in workflows and subscriptions. Users must already be defined in the system before you can assign the users to an alias.

Creating Aliases

Use the User Admin tool to create aliases. You must belong to the Admin role to create an alias.

1. Select the **Aliases** tab on the User Admin screen and click **Add**.

   The Add New Alias screen is displayed.

2. Type **All** in the **Alias Name** field and **All Employees** in the **Description** field.

3. Click **Add**. The Select Users screen is displayed.

4. Select **jdoe** from the **Users** list and click **OK**. The user **jdoe** is displayed in the **Users** list of the Add New Alias screen.

5. Click **OK**.

EXERCISE 2: ADDING GROUPS, ROLES, AND USERS

This exercise consists of the following tasks:

1. Add the following security groups to Content Server.

Group Name	Description
Marketing	Marketing Project Teams
Confidential	High Level Access
Accounting	General Accounting

2. Add the following roles to Content Server. Permissions listed are in addition to the default Read access to the Public group.

Role Name	Rights	Permissions
AccountingAdmin	Right.Apps.UserAdmin, Rights.Apps.Workflow	R, W, D to Accounting group
AcctContributor	None	R, W to Accounting group
ConfidentialContributor	None	R, W, D to all groups except Public
HRContributor	None	R, W to HR group
MktAdmin	Right.Apps.UserAdmin, Rights.Apps.Workflow	R, W, D, A to Marketing group
MktContributor	None	R, W to Marketing group

3. Add the following users to Content Server. The Authorization Type for each user should be **Local**. Use **idc** as the password for each user. Remember that the password is case sensitive.

Name	Full Name	Assigned Roles
jsmith	John Smith	AccountingAdmin
bjones	Bill Jones	HRContributor
sjames	Shawn James	ConfidentialContributor
swilson	Sally Wilson	AcctContributor, HRContributor
tadams	Tom Adams	MktContributor
pkelly	Pat Kelly	MktContributor
krandall	Kim Randall	MktAdmin, AcctContributor

4. Add each user to the **All Employees** alias.

5. Create an alias called **MktTeam**, and add the Marketing group members (tadams, pkelly, and krandall) to it.

PERFORMANCE CONSIDERATIONS

When defining the number of security groups, there are two areas of performance you need to keep in mind:

❖ Search Performance (page 3-20)

❖ User Admin Performance for Local Users (page 3-20)

Because performance is subjective, we can give you only guidelines in this area. In addition, the server hardware configuration that you are running on also affects performance.

Important: The guidelines given here are the results of performance testing run on a PC with a 400 MHz processor, 128 MB of RAM and using Microsoft Access as the SQL database.

Search Performance

Search performance is affected by the number of security groups to which a user has Read permission.

The more security groups to which a user has permission, the slower the search performance. The following table serves as a guideline:

No. of Security Groups	Factor of Increase in Seconds
1	x (where x = the number of seconds to perform search)
10	2x
20	3x
30	4x

User Admin Performance for Local Users

The total number of security groups times the total number of roles determines the number of roles in the RowDefinition table, and affects the performance of the User Admin functions for operations involving local users. To determine the approximate time to perform an operation within the User Admin screen, such as adding a security group or changing permissions for a role, use the formula:

$$\frac{(\text{Number of Security Groups}) \times (\text{Number of Roles})}{1000} = \text{Time of operation in seconds}$$

For example, using the hardware configuration described earlier, it took approximately 10 seconds to add a security group and/or role when the RowDefinition table equaled 10,000.

As the number of security groups increases, administration performance is affected more than a user searching for content.

You can now proceed with Tutorial 3: Accounts (see Chapter 4).

ACCOUNTS

OVERVIEW

This section covers these topics:

It is recommended that you go through this tutorial from beginning to end, in the suggested order.

ABOUT ACCOUNTS

An account is a metadata field that is filled out when content is checked in. A user must have the appropriate privilege to the account to access the content. Once activated, accounts become the primary security on the security group. Accounts can provide greater flexibility and granularity than security groups alone.

This section covers these topics:

❖ Accounts Compared to Security Groups (page 4-2)

❖ Performance (page 4-4)

Accounts Compared to Security Groups

Security groups use the "Library" model, offering broad access control. For example, a library provides access to content (books, reference material, and periodicals) arranged by information, not by a user.

Accounts use the "Bank" model, offering thousands of accounts with limited user access. Similarly, accounts are centered more on the user than information.

Accounts imply a hierarchy of permissions. Users at the bottom of the hierarchy have access to few accounts. Users at the top of the hierarchy can have broad access to the account structure. For example, a company finds that too many security groups are necessary to provide the security they need. Accounts can resolve it. In general, activate accounts if you need more than 50 security groups.

Suppose the following scenario:

❖ Ruggans Financial has 50 locations worldwide, including Minneapolis (MSP), Boston (BOS), and Denver (DEN).

❖ Each location has 12 departments, including Human Resources (HR), Customer Service (CS), and Information Services (IS).

❖ Some content can be seen by HR at any location as shown in the diagram below.
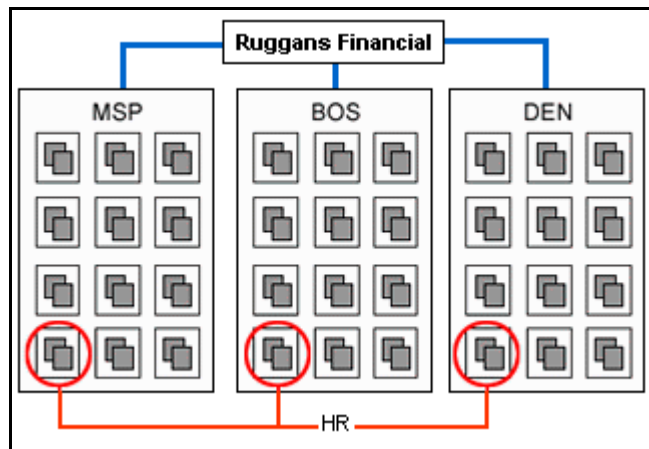
❖ Some content can only be seen by HR in the MSP location. This means HR users from other locations cannot see the content in the MSP account as shown in the diagram below.
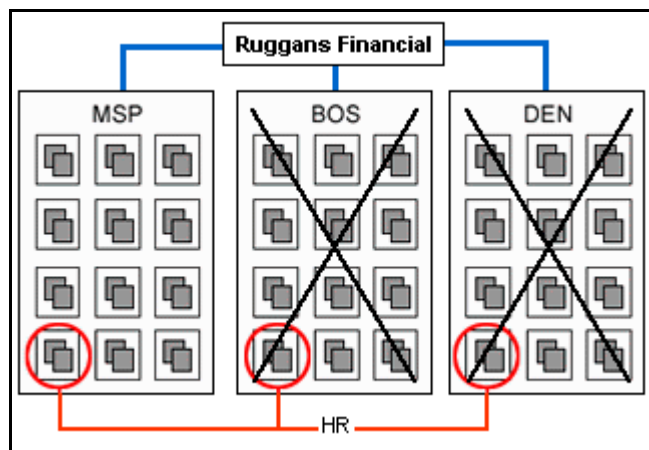
To accomplish the required security in this example without using accounts, each department in each location would be a different security group. This is a total of 600 security groups (50 locations times 12 departments), which exceeds the recommended limit.

If we used accounts and set up one account for each location, we would have 50 Accounts but only 12 security groups, one for each department.

Performance

You can create an unlimited number of accounts. However, as with security groups, search performance is affected. A search will take approximately 0.1 second for every account assigned to a user; a search done by a user who is assigned 10 accounts would take approximately 1 second.

Because performance is subjective, we can give you only guidelines in this area. In addition, the server hardware configuration that you are running on also affects performance.

ACCOUNTS AND PERMISSIONS

With accounts, access to content is determined by the intersection of a user's permissions and the user's security group. For example, a user with Read/Write permission to the security group and Read/Write/Delete permissions to the account will have Read/Write permission to the content in the security group matching their account.

This section covers these topics:

Security Group Only Model
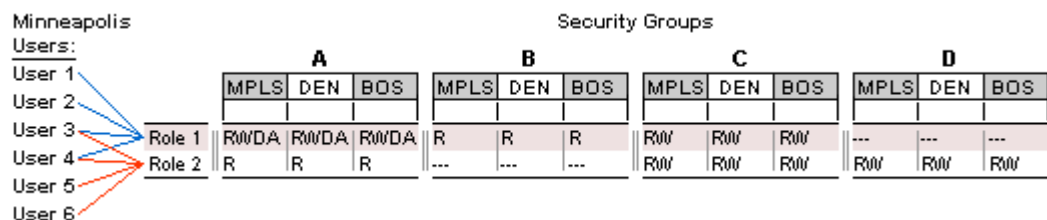
In the preceding illustration, Minneapolis Users 1 through 4 have Role 1, giving them the following permissions in all locations:

❖ Read/Write/Delete/Admin permission to all content in security group A

❖ Read permission to all content in security group B

❖ Read/Write permission to all content in security group C, and

❖ No permission to content in security group D.

Security Group With Accounts Model
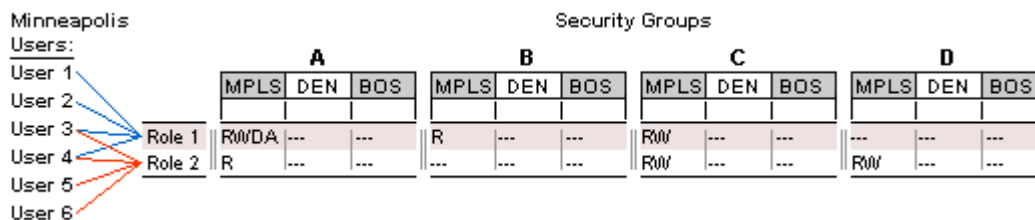
In the preceding illustration, three accounts are added to the security model, based on location: Minneapolis, Denver, and Boston. The content within each security group is further categorized by account. Minneapolis Users 1 through 4 are given permission only to the Minneapolis account.

For ease of explanation, we looked at a user with only one role. Users can have more than one role and more than one account assigned to them. If Role 2 is added to User1, an additional RW permission is granted to the MSP content in Security Group D (the permissions overlap). To get access to DEN or BOS, the account needs to be added to the user's permissions.

Hierarchical Account Scenario

Currently, all Ruggans content is in the Public security group, to which all departments have access. For this tutorial, it is necessary that only Marketing Department employees have access to marketing content. Also, each Marketing Department employee should be able to view only the projects they are working on and not other projects. Shawn James, the marketing manager, needs access to all Marketing Department projects. Tom Adams needs access to technical information for Project A. Pat Kelly needs access to all information on Project B. And Kim Randall needs access to the cost information for both projects. The account hierarchy should look like the following figure:
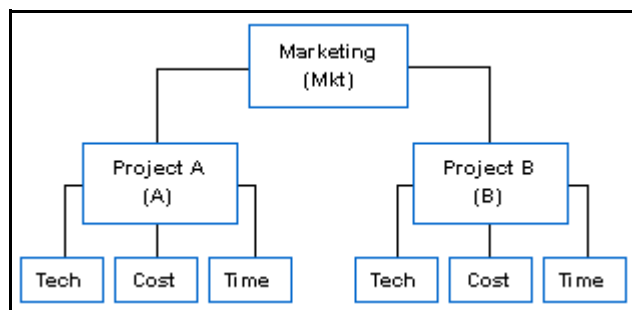
You would need to create nine accounts to handle this security model. We will abbreviate to make the account names short.

- Mkt	- Mkt/A/Cost	- Mkt/B/Tech
- Mkt/A	- Mkt/A/Time	- Mkt/B/Cost
- Mkt/A/Tech	- Mkt/B	- Mkt/B/Time

❖ The Mkt account gives permission to all projects: Project A, Project B, and the sub-accounts under both projects (Tech, Cost, and Time). Shawn James should get access to this account.

❖ The Mkt/A/Tech account gives permission to any content checked into the Tech account for Project A. Tom Adams should get access to this account.

❖ The Mkt/B account gives permission to all content checked into the Project B account and its sub-accounts: Tech, Cost, and Time. Pat Kelly should get access to this account.

❖ The Mkt/A/Cost and Mkt/B/Cost accounts give permission to cost information for both projects. Kim Randall needs access to both accounts.

ACCOUNT NAMING CONVENTIONS

This section covers these topics:

❖ General Conventions (page 4-7)

❖ Using Slashes In Account Names (page 4-8)

❖ Using Accounts with Microsoft Network Security (page 4-9)

General Conventions

When designing your account naming conventions, keep the names short and hierarchical. Hierarchical naming conventions are recommended for versatility.

Short, consistent names are recommended so that they are easy to remember and use. For example, if you are creating accounts by location—for example, Minneapolis, Denver, Boston, and London— you could use the airport codes MSP, DEN, BOS, and LGW (Gatwick), respectively.

Account names can be a maximum of 30 characters. The following characters are not acceptable: spaces, tabs, linefeeds, carriage returns and the symbols ; : ^ ? : @ & + " # % < > * ~ |

Tech Tip: Document the naming convention for your accounts and how they are used. This will help the users and sub domains.

Using Slashes In Account Names

Slashes (/) in account names tell Content Server how to organize and store the permission information in the file structure. Content Server automatically generates the folder names for accounts based on the slashes, and identifies all account folders with the prefix @. Slashes are optional, but are recommended for ease of file maintenance.

The following figure shows how Content Server would store the Ruggans accounts in the file structure:

When slashes are used:
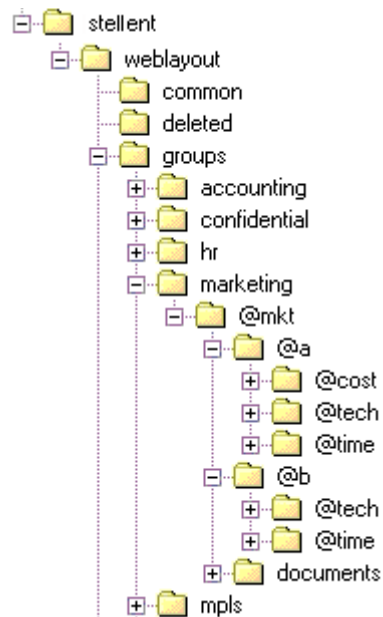
When slashes are not used:
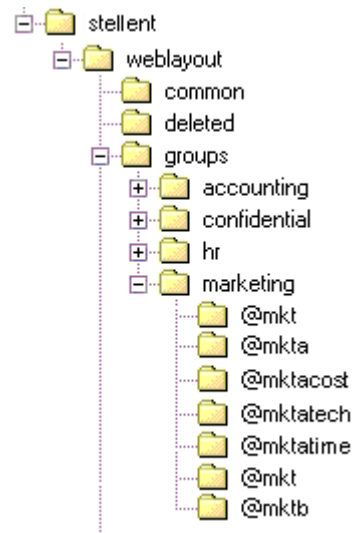
Caution: Highly complex nested directories can slow the performance of programs that span the directory structure, such as backup software or the Archiver screen.

Using Accounts with Microsoft Network Security

When using Microsoft Network Security, account names cannot have slashes (/) in them. If you were using Microsoft Network security, the Ruggans accounts could be named without the slash as follows:

- Mkt	- MktB
- MktA	- MktBTech
- MktATech	- MktBCost
- MktACost	- MktBTime
- MktATime	

Tech Tip: For clarity, consider using an underscore (_) to help define the account structure. For example, Mkt_A_Tech. Keep in mind that you have a 30-character limit and the underscore counts as one character.

ACTIVATING ACCOUNTS

This section covers these topics:

❖ Editing the Configuration File (page 4-9)

❖ Admin Server Configuration Options (page 4-10)

❖ Restarting the Server (page 4-11)

❖ Verifying That Accounts Are Active (page 4-11)

Editing the Configuration File

To activate accounts, you must edit the Content Server configuration file. The config.cfg file can be edited using a text editor such as WordPad, as you did in the introduction to these tutorials, or on the Admin Server page, which is accessed from the Administration tray.

1. Click **Administration** in the tray area to open the tray, and click **Admin Server**. The Administration for Servers page is displayed.

Figure 4-12 Administration Tray
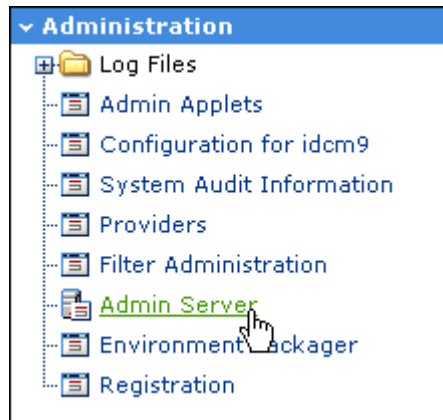
2. Click the Content Server instance for which you want to enable accounts. If you have more than one Content Server instance, you will see a button for each.

Admin Server Configuration Options

The following screen shows you the options for configuring the content server.

1. Click **General Configuration**. The General Configuration screen is displayed.

2. Scroll to the bottom of the screen. The *config.cfg* file is displayed in the **Additional Configuration variables** field.

3. Scroll to the bottom of the field and type **UseAccounts=true**.

Important: The *config.cfg* file is case sensitive. Make sure that spelling, case, and spacing is correct.

4. Click **Save**.
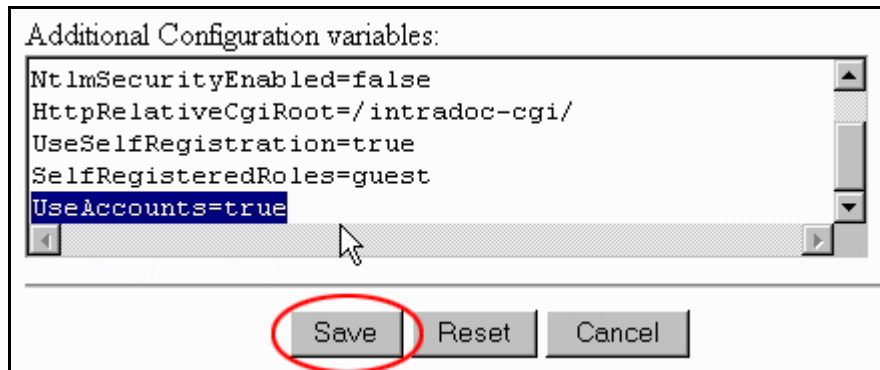
Restarting the Server

You must restart the content server before any configuration changes will take effect. In the lower left corner of the Configuration Options page, you will see a reminder to restart the server.
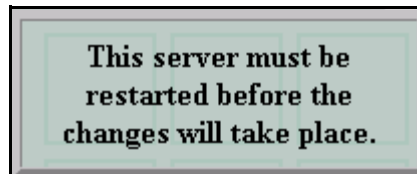
1. Click the circular arrow to restart the content server.

The restart reminder will no longer be displayed.

2. After the content server has restarted, click **Administration**. The Administration page is displayed.

Verifying That Accounts Are Active

To verify that accounts are active, complete the following steps:

1. Click **User Admin** on the Administration page.

2. Pull down the **Security** menu.

Predefined Accounts is listed as an option.
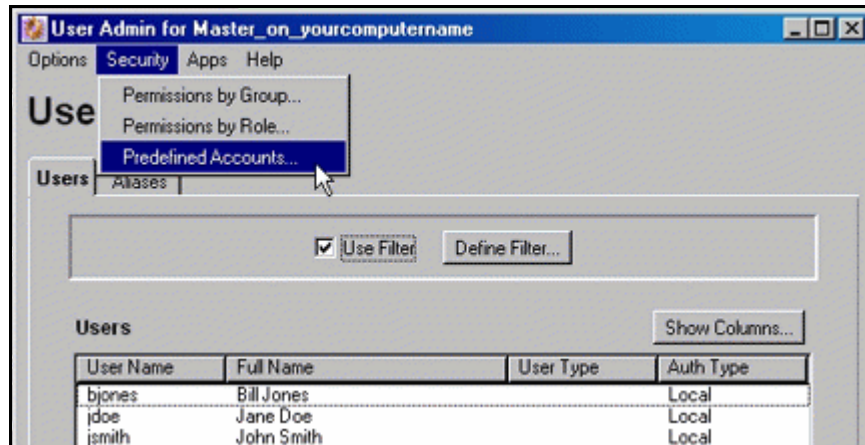
3. If you do not see Predefined Accounts listed as an option on the Security menu:

   a. Return to the Admin Server General Configuration page.

   b. Verify that you typed **UseAccounts=true** accurately at the end of the config.cfg file.

   c. Verify that your edits were saved.

   d. Restart the content server again.

CREATING ACCOUNTS

Accounts can be predefined using the Security menu in the User Admin screen, or they can be created dynamically when users type in an account name as they check in content.

Creating predefined accounts makes it easier for the users. They can select an account from a drop down list instead of typing it in. Once created, accounts appear in the following places:

❖ A choice list for Accounts on the Content Check In Form page

❖ A choice list for Default Accounts on the User Admin screen

Create predefined accounts for locations and departments as follows:

1. From the User Admin screen, select **Security—Predefined Accounts**.

2. Click **Add**.

3. Enter **BOS** in the **Predefined Account** field and click **OK**.

4. Click **Add**.

5. Enter **MSP** in the **Predefined Account** field and click **OK**.

6. Click **Add**.

7. Enter **DEN** in the Predefined Account field and click **OK**.

8. Continue adding the following accounts:

- Mkt	- Mkt/A/Cost	- Mkt/B/Tech
- Mkt/A	- Mkt/A/Time	- Mkt/B/Cost
- Mkt/A/Tech	- Mkt/B	- Mkt/B/Time

9. Click **Close** to exit the Predefined Accounts screen.
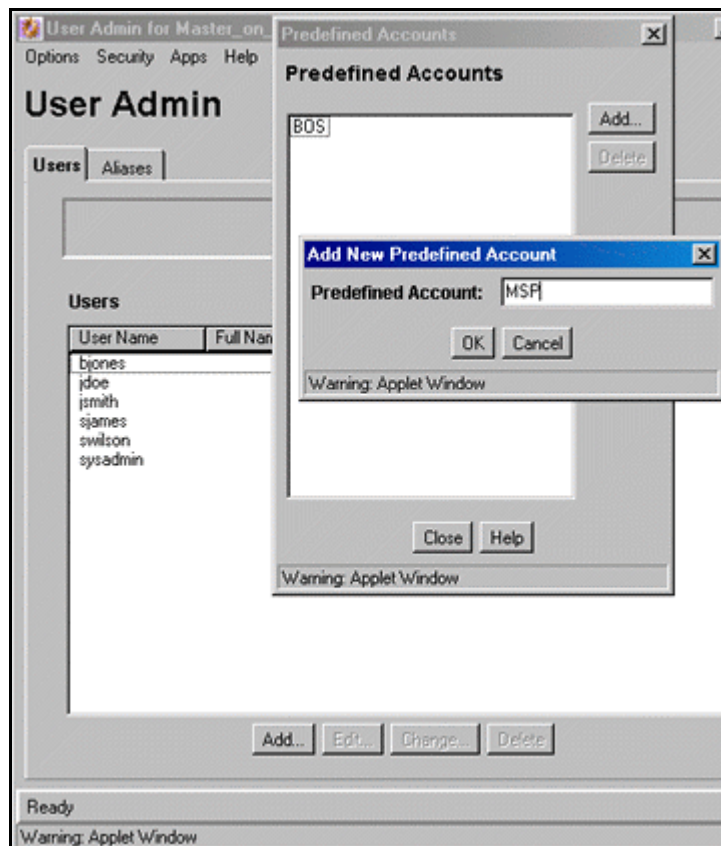
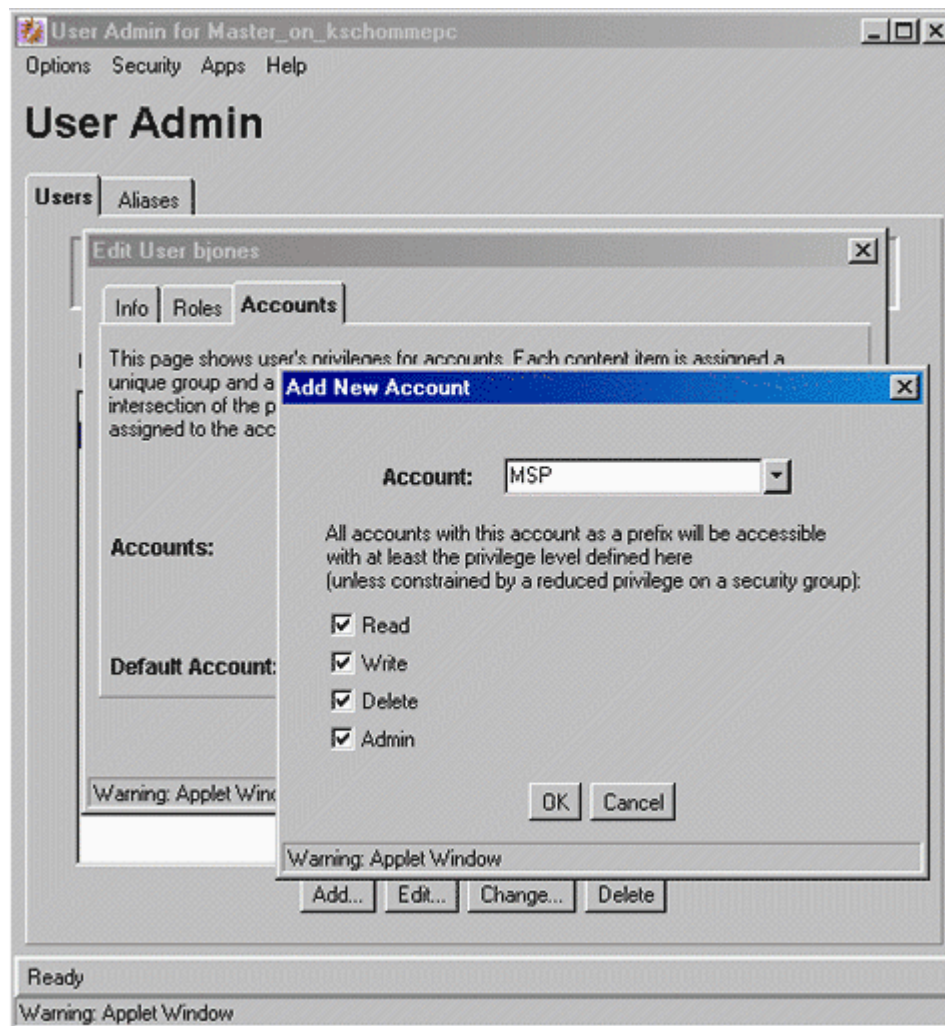# ASSIGNING ACCOUNTS TO USERS

Assign the accounts you just created to users and test that the accounts are working properly.
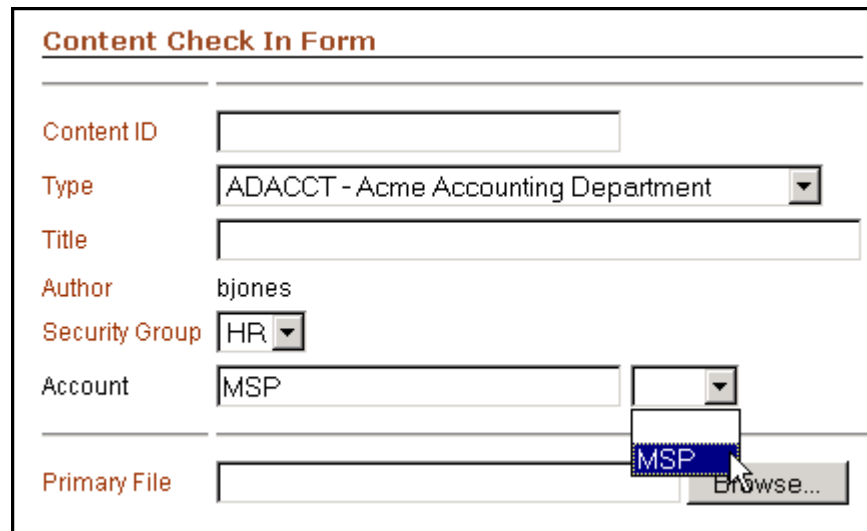
From the User Admin screen:

1. Select **bjones** from the user list.

2. Click **Edit**.

3. Select the **Accounts** tab.

4. Click **Add**, select **MSP** in the **Account** choice list, and click **OK**.

5. Select **MSP** in the **Default Account** choice list and click **OK**.

6. Open a new browser instance and login as *bjones* (password: **idc**).

7. Click **Content Manager** and then **New Check In**. Notice that only MSP is visible in the **Account** choice list.

SPECIAL ACCOUNT TYPES

There are two special account types that are predefined in Content Server. These special accounts make it easier to set up the proper permissions as defined below.

Classification	Description
[documents without accounts]	This type defines what permission a user has on all content checked in without an account. By default, users have Read/Write/Delete/Admin to [documents without accounts]. The permissions you have is the intersection between the permissions given to [documents without accounts] and the security groups your roles give you permission to.
[all accounts]	This type defines what permission a user has on all content checked in with an account. The permissions you have is the intersection between the permissions given to [all accounts] and the security groups your roles give you permission to.

EXERCISE 3: CHECKING IN CONTENT WITH ACCOUNTS

This exercise consists of the following tasks:

1. Assign accounts to the following users. Specify the first account listed here as the default account.

User	Account	Privileges
Bill Jones	MSP	All
Jane Doe	BOS, DEN	All
John Smith	BOS, MSP, DEN	All

User	Account	Privileges
Kim Randall	MSP, BOS, Mkt/A/Cost, Mkt/B/Cost	Read, Write
Pat Kelly	MSP, Mkt/A	Read, Write
Shawn James	MSP, BOS, DEN, Mkt	All
Sally Wilson	DEN, Mkt	All
Tom Adams	MSP, Mkt/A/Tech	Read, Write

2. Open a new browser instance, login as **bjones** (password: idc), and check in the following content, which is located in the Ruggans Tutorial Files/Content folder. Leave the **Type** set to the default. Close the browser instance when you are finished.

Content ID	Title	Author	Security Group	Account
006	006_hr	Bill Jones	HR	MSP
007	007_hr	Bill Jones	HR	MSP

3. Open a new browser instance, login as **jdoe** (password: idc), and check in the following content. Notice that Jane Doe has two accounts listed in the Account choice list. Leave the **Type** set to the default. Close the browser instance when you are finished.

Content ID	Title	Author	Security Group	Account
008	008_hr	Jane Doe	HR	DEN
009	009_hr	Jane Doe	HR	DEN
010	010_hr	Jane Doe	HR	BOS

4. Open a new browser instance, login as **sysadmin** (password: idc), and check in the following content. Notice that as the system administrator, you have access to all users in the **User** choice list, and all accounts in the **Account** choice list. Leave the **Type** set to the default. Close the browser instance when finished.

Content ID	Title	Author	Security Group	Account
011	011_conf	Shawn James	Confidential	BOS
012	012_conf	Shawn James	Confidential	BOS
013	013_conf	Shawn James	Confidential	DEN
014	014_conf	Shawn James	Confidential	DEN
015	015_conf	Shawn James	Confidential	MSP
016	016_acct	Sally Wilson	Accounting	Mkt/A/Cost
017	017_acct	Sally Wilson	Accounting	Mkt/B/Cost
018	018_acct	John Smith	Accounting	BOS
019	019_acct	Sally Wilson	Accounting	DEN
020	020_acct	John Smith	Accounting	MSP
021	021_mkt	Pat Kelly	Marketing	Mkt/A/Time
022	022_mkt	Shawn James	Marketing	Mkt/B/Time
023	023_mkt	Pat Kelly	Marketing	Mkt/A/Tech
024	024_mkt	Shawn James	Marketing	Mkt/B/Tech
025	025_mkt	Sally Wilson	Marketing	Mkt

VERIFYING ACCOUNT ACCESS: SHAWN JAMES

Earlier you were shown a hierarchical account scenario in which Shawn James needed access to all Marketing projects, Tom Adams needed access to technical information for Marketing Project A, Pat Kelly needed access to all information on Project A, and Kim Randall needed access to the cost information for both projects. Verify that these people now have the access that they need.

1. Open a new browser instance and login as Shawn James (User Name: **sjames**, password: **idc**).

2. Click **Search**.

3. Select **Mkt** from the **Account** choice list.

4. Click **Search**.

   The following content list should be displayed:

ID	Title	Date	Author	Actions
017	017_acct	9/8/03	swilson	
016	016_acct	9/8/03	swilson	

Search Results — Found 2 items matching the query. Actions: Select an action

These two files are the cost information for Projects A and B. No other marketing content has been found, but Shawn James should have permission to files with content IDs 021 through 025 as well.

Why is no other marketing content displayed? *(Continued in next subsection...)*

PERMISSIONS LESS PRIVILEGES

Remember that when using accounts, access to content is determined by the intersection of a user's permissions and a user's security group.

No other content was found for Shawn James because even though he has access to all of Marketing's accounts, he does not have access to the Marketing security group.

1. Open a new browser session and login as **sysadmin**.

2. Open the Administration tray and click **Admin Applets**.

3. Click **User Admin**.

4. Select **sjames** and click **Edit**.

5. Select the **Roles** tab and click **Add Role**.

6. Select **MktContributor** from the choice list and click **OK**.
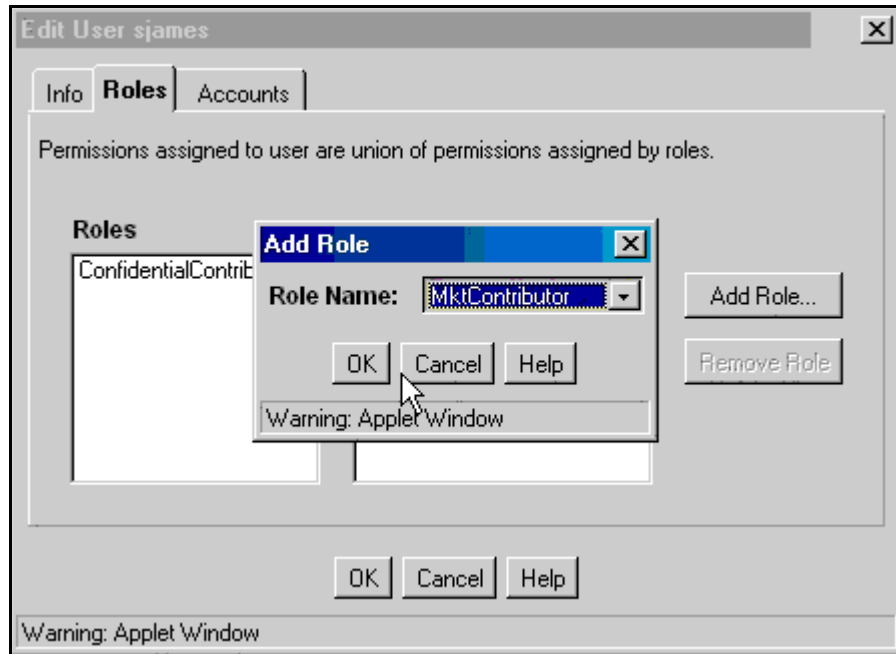
7. Click **OK** to close the Edit User screen, and close the User Admin screen.

8. Open a new browser instance, login as **sjames**, and search for content assigned to the Mkt account. You should now see the additional files.

VERIFYING ACCOUNT ACCESS: PAT KELLY

Pat Kelly needs access to Project A information only.

1. Open a new browser instance and login as Pat Kelly (User Name: **pkelly**, password: **idc**).

2. Click **Search**.

3. Pull down the **Account** choice list.

    Pat Kelly has access to only Project A information.

EXERCISE 4: VERIFYING USER ACCESS

Open up a new browser session for each user and search for content based on their security groups. Search on each security group except Public. The user name, security group, account, and expected results are provided.

User Name	Security Group	Account	Search Results
bjones	HR	MSP	006_hr, 007_hr
jdoe	HR	BOS, DEN	008_hr, 009_hr, 010_hr

User Name	Security Group	Account	Search Results
jsmith	Accounting	BOS, MSP, DEN	018_acct, 019_acct, 020_acct
krandall	Accounting, Marketing	MSP, BOS, Mkt/A/Cost, Mkt/B/Cost	016_acct, 017_acct, 018_acct, 019_acct, 020_acct
swilson	Accounting, HR	DEN, Mkt	019_acct, 008_hr, 009_hr
tadams	Marketing	MSP, Mkt/A/Tech	023_mkt

If you do not receive the expected results:

1. Login as **sysadmin**.

2. Open the **User Admin** screen from the Administration page.

3. Verify that the user belongs to the correct security group and has the correct accounts assigned.

If you still do not receive the expected results:

1. Login as **sysadmin**.

2. Search for the content missing from the expected results.

3. Click **Info** (i) .
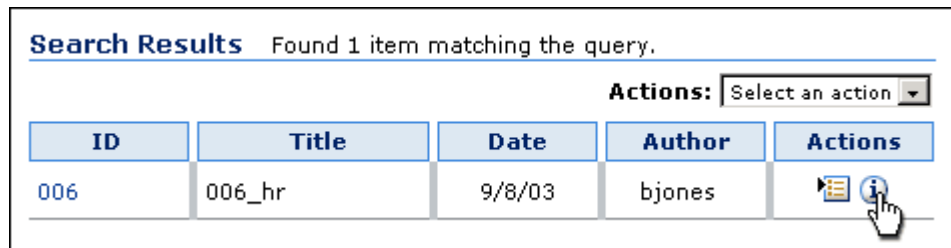
4. Verify that the document has been checked in to the right security group and account.

Content Information

Actions: [Select an action ▼]

Content ID : 006
Revision: 1
Type: ADACCT - Acme Accounting Department
Title: 006_hr
Author: bjones
Comments:
Security Group: HR
Account: MSP
Checked Out By:
Status: Released
Formats: application/msword

If the security group or the account information is incorrect:

1. Select **Update** from the Actions drop-down menu.

2. Make the corrections and click **Submit Update**.

Info Update Form

Content ID	006
Type	ADACCT - Acme Accounting Department ▼
Title	006_hr
Author	bjones	bjones ▼
Security Group	HR ▼
	Accounting
	Confidential
	HR
Account	Marketing
	Public
	Secure
Revision	
Comments	
Release Date	9/8/03 4:13 PM
Expiration Date	

[Submit Update] [Reset] [Quick Help]

You can now proceed with Tutorial 4: Library Folders (see Chapter 5).

5

LIBRARY FOLDERS

OVERVIEW

This section covers these topics:

BUILDING THE LIBRARY FOLDER HIERARCHY

Your Library Folder hierarchy is built using the Web Layout Manager admin applet. It determines how content is organized in your Library Folders under the Browse Content tray and provides a convenient and intuitive way for people to find the information they need. You can design the hierarchy to access all content or only the most commonly accessed content.

This section covers these topics:

Page Links

There are three types of links used to develop your Library hierarchy.

| Name	Description
Local Page	A Local Page is a link to a static page. This page will have a physical file associated with it, identified by a Page Name. By default, the Table of Contents page has the Page Name *index*. You will see this as you start building the web site. A Local Page can also be defined as an Active or Historical Report.
Query	A Query is a link to a dynamic search result. When you click on the link, it queries the search index for all content that meets the predefined criteria. The criteria are defined by one or more Info Fields that you, as system administrator, establish. As content meeting the criteria is checked in to Content Server, it will be displayed when the query link is used.
External URL	An External URL is a link to a specified URL address. You can link to any URL address on the Internet, on an Extranet, or on an Intranet. The full HTTP address must be specified. For example, the full HTTP address to Oracle's home page is http://www.oracle.com.

A typical hierarchy involves a link in the Library folders under the Browse Content tray to a local department page that has links to queries for specific content. For example, a link

called Human Resources in the Library folders would take a user to a local page with links called Forms and Policies, Benefit Info, and Resumes. Each of these links would query the search index and return a listing based on the type of content it is: Form, Benefit, or Resume.

You can also establish custom metadata fields and use them to refine your content query. In this tutorial, you will be shown how to create content types and custom metadata fields specific to your needs.

As you design your hierarchy, think of how your users would find particular content. Draw out the hierarchy structure to help you develop it.

Figure 5-1   Example of Hierarchy Diagram
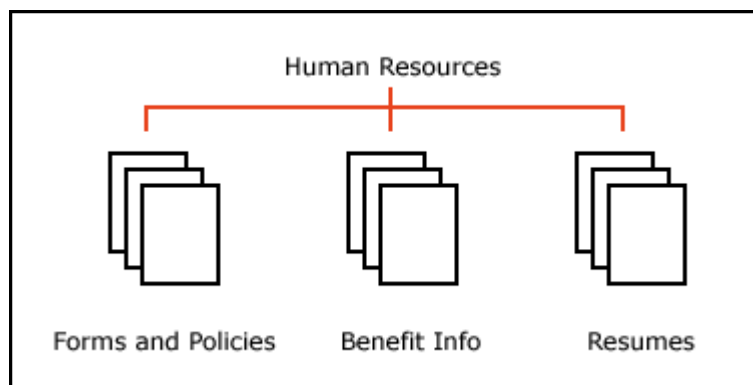
Restricting Access to the Library Hierarchy

To restrict access to content displayed on a page by security group, enable **Restrict content queries by security group** when adding a page using the Web Layout Manager admin applet. To restrict access by account, enable **Restrict content queries by account**. By default, queries on the same local page are restricted by security group.

Figure 5-2   Security Restriction Settings on Add Web Page screen

CONTENT TYPES

When you check content into Content Server, you must specify the content type on the Content Check In Form. Until now, you have used the default type. To create library folder searches based on content type, you define types useful to your business.

This section covers these topics:

❖ Defining Content Types (page 5-5)

❖ The Configuration Manager (page 5-6)

❖ Deleting Types (page 5-6)

❖ Adding Types (page 5-7)

❖ Exercise 5: Adding Types (page 5-9)

Defining Content Types

Types are identifiers used to group content on the web site. For flexibility, keep the following points in mind when defining types:

❖ Create types to divide content into manageable groups

❖ Keep types general

❖ Keep the number of types small so that the choice list is manageable

There are three aspects of a type that must be specified:

Name	Description
Type Name	The Type Name is the identifier used to group content on the web and is available from the Type choice list on the Content Check In Form. For example, if you create a type called HRresumes and check in all resumes as that type, you can define a query link based on the HRresumes type that finds all resumes. Maximum field length is 30 characters, although the following are not acceptable: spaces, tabs, linefeeds, carriage returns and the symbols: ; ^ ? : @ & + " # % < > * ~ |
Description	The Description field is a description of the type. The Description will appear next to the Type Name on the Content Check In Form and Search page choice lists. Maximum field length is 80 characters.
GIF	The GIF is an image that represents the type. Select one from the default list or develop your own. To make custom GIFs available to the Configuration Manager, copy them to following directory: *\stellent\weblayout\images\docgifs*.

The Configuration Manager
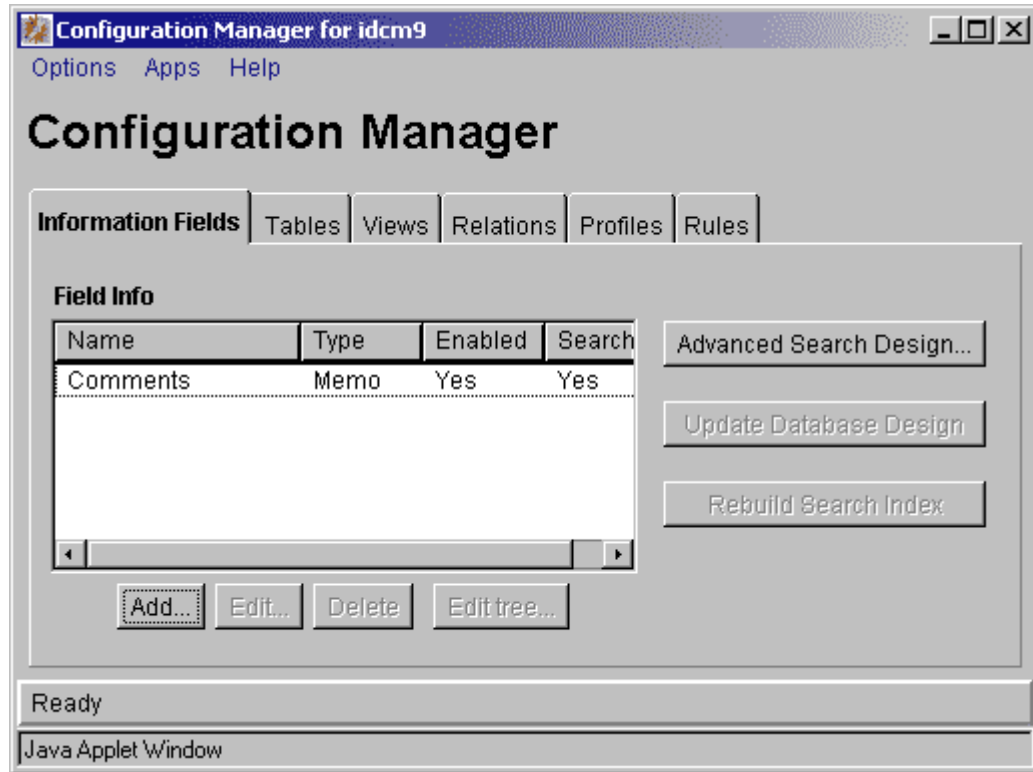
Types are created using the Configuration Manager screen, which is accessed from the Administration Applets page.

Open the Configuration Manager now.

1. Open the Administration tray and click **Admin Applets**.

2. Click **Configuration Manager** on the Administration Applets page. The Configuration Manager screen is displayed.

Deleting Types

Content Server comes with seven predefined types to use as examples. You can keep these types or delete them as you create types specific to your company.

1. Display existing types by selecting **Options—Content Types**.

2. Select the first type listed, **ADACCT**, and click **Delete**.

    A delete confirmation screen is displayed.

3. Click **Yes**.

   A notification screen is displayed explaining that there are files of this type checked into the system. Content Server will not allow you to delete types that are in use.
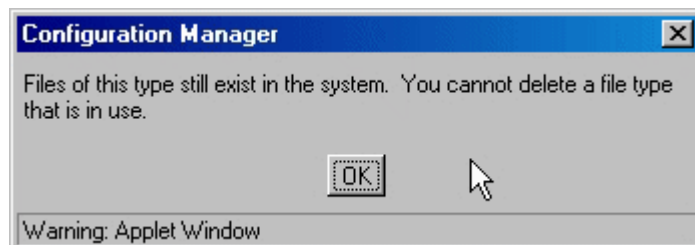
4. Click **OK**.

5. Select the second type, **ADCORP**, and click **Delete**, then click **Yes** on the confirmation screen to delete the type.

   The type is deleted from the system and is no longer listed in the Configuration Manager screen.

6. Repeat step 4 with each remaining type until only the **ADACCT** type is listed.

Adding Types

To add content types, complete the following steps:

1. Make sure the Content Types screen is displayed. To display the Content Types screen, select **Options—Content Types.**

2. Click **Add**.

   The Add New Content Type screen is displayed.

3. Type **HRresume** in the Name field.

4. Type **All Resumes** in the Description field.

5. Select **persdoc.gif** from the GIF choice list.

   A preview image of the GIF you selected is displayed next to the choice list.

6. Click **OK**.

Figure 5-3   Add New Content Type screen

The HRresume type is now listed in the Configuration Manager screen.

Figure 5-4   Configuration Manager screen with HRresume type listed
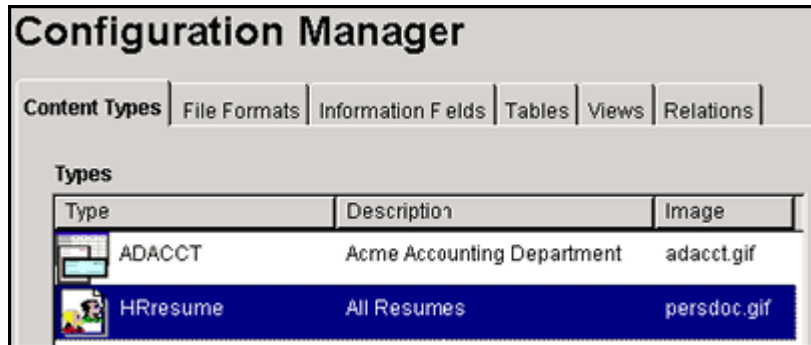
Note: You can always go back and edit the description or GIF of a type, but you cannot change the name without deleting it first and adding it back in.
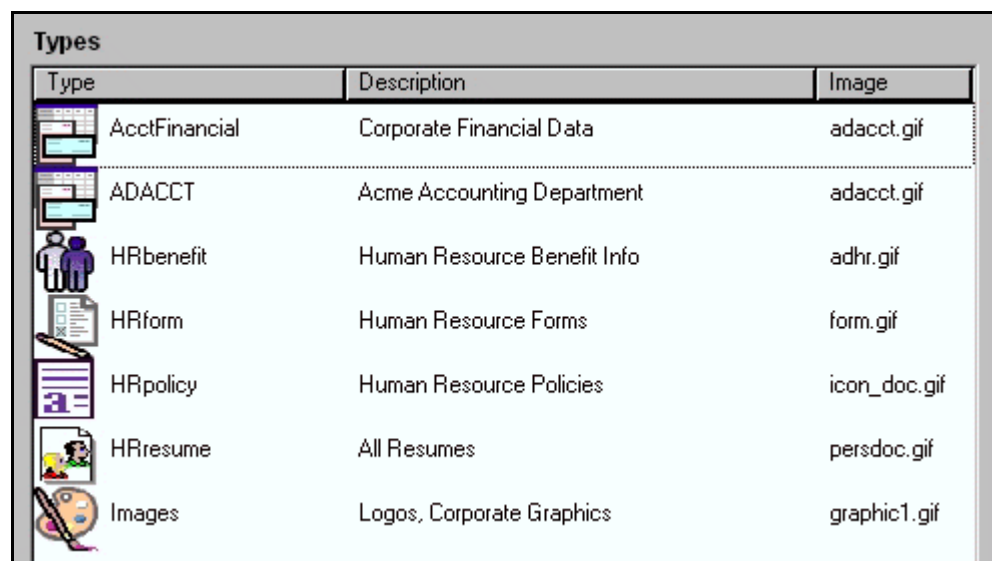
Exercise 5: Adding Types

This exercise consists of the following tasks:

1.   Add five more types using the Configuration Manager screen:

Type Name	Description	GIF
HRform	Human Resource Forms	form.gif
HRpolicy	Human Resource Policies	icon_doc.gif
HRbenefit	Human Resource Benefit Info	adhr.gif
Images	Logos, Corporate Graphics	graphic1.gif
AcctFinancial	Corporate Financial Data	adacct.gif

When you have finished, the following types should be listed in the Configuration Manager screen:

> **Tech Tip:** Listing the department initials or some other organizing group in the type name helps to organize the types in the choice list on the Content Check In Form. For example, by preceding **benefit, form**, and **policy** with the initials **HR**, people in the HR department can more quickly find the type they need.

Check in the following content, which is located in the *Ruggans Tutorial Files/Content* folder. Assign each item to the **Public** security group and leave the **Account** field empty.

Content ID	Title	Author	Type
026	026_form	Bill Jones	HRform
027	027_form	Bill Jones	HRform
028	028_pol	Bill Jones	HRpolicy
029	029_ben	Bill Jones	HRbenefit
030	030_res	Bill Jones	HRresume

DESIGNING AND CREATING CUSTOM METADATA FIELDS

Files are stored in a central repository where you can check them in and out. You can easily add custom metadata fields to capture information for each file. The custom information is similar to the information in a library card catalog and helps users search for the file. For example, a file description can include a part number, a department, a location, or a project. Any number of these fields can be included as custom attributes.

This section covers these topics:

❖ Standard Info Fields (page 5-11)

❖ Defining Custom Metadata Fields (page 5-12)

❖ Adding a Custom Metadata Field (page 5-15)

❖ Updating the Database Design and Search Index (page 5-17)

❖ Viewing the New Custom Field (page 5-18)

Standard Info Fields

There are 11 standard metadata fields that come pre-configured with Content Server:

Field	Description
Content ID	The Content ID is a unique identifier.
Type	The Type is an identifier used to group files.
Title	The Title is a descriptive name identifying the file.
Author	The Author is the person who created or revised the file.
Security Group	The Security Group is a set of files with the same access privileges.
Primary File	The Primary File is the pathname to the original file being checked in.
Alternate File	The Alternate File is the pathname to another web-viewable file format.

Field	Description
Revision	The Revision number represents how many times this file has gone through its life cycle.
Comments	The Comments field is for additional information about the file.
Release Date	The Release Date is the date that the file gets published on the Web.
Expiration Date	The Expiration Date is the day the file is removed from the Web site.

Defining Custom Metadata Fields

Custom metadata fields will appear on the following Content Server pages:
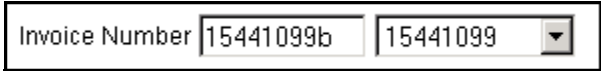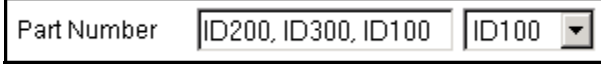
❖ Content Check In Form (New and Revised)

❖ Search

❖ Content Information

❖ Info Update Form

The following are the parameters that define a custom metadata field:

| Field	Description
Field Name	The Field Name is the name that Content Server uses to identify the custom metadata field. The maximum length is 28 characters and may only contain the following characters: Letters (a-z), numbers (0-9) and underscore (_). The first character in the name must begin with a letter.
Field Caption	The Field Caption is the label for the field that displays on Content Server pages.

Field	Description
Field Type	The Field Type defines the length and function of the field. **Text:** 30 characters maximum. **Long Text:** 100 characters maximum. **Date:** *dd/mm/yyyy* or *dd/mm/yy*. **Memo:** 255 characters maximum. **Integer:** -2^{31} to 2^{31} (-2 billion to +2 billion). By definition, an integer is a natural number, so decimal values and commas are not permitted.
Field Order	The Field Order is the sequence in which the field is displayed on Content Server pages. Starting at 2, the number automatically increments as new fields are added.
Require Value	Require Value prevents files from being checked in if the field does not contain a value.
Enable on User Interface	Enable for Search Index allows the search engine to index the field, and the field becomes searchable.
Enable for Search Index	Enable for Search Index allows the search engine to index the field, and the field becomes searchable.
Enable Option List	Enable Option List creates a user-selectable choice list on Content Server pages.

| Field	Description
Option List Type	The Option List Type specifies the type of choice list: **Select List Validated**—For Batch Load and Archiver/Replicator purposes, this option ensures that only files whose specified values are current options for this field are checked in. **Select List Not Validated**—For Batch Load and Archiver/Replicator purposes, this option permits check in of files whose specified values are not current options. **Edit and Select List**—Provides both a text field and a choice list. Contributors can enter values that are not in the choice list. **Figure 5-5** Example Invoice Number 15441099b 15441099 **Edit and Multiselect List**—Provides both a text field and a choice list. Contributors can enter values that are not in the choice list. Additionally, they can select or enter multiple values. **Figure 5-6** Example Part Number ID200, ID300, ID100 ID100
Default Value	The Default Value is the value that automatically populates the field. A default value is not required.
Option List Key	The Option List Key is the name of the list of values that appear in the choice list. By default, this name is generated from the Field Caption. An option list key can be used for more than one field.
Edit (Option List Key)	Allows the choice list values to be added, edited, deleted, and sorted.

Adding a Custom Metadata Field

Custom metadata fields are created using the Configuration Manager screen.

1. Click **Configuration Manager** on the Administration page. The Configuration Manager screen is displayed

2. Click the **Information Fields** tab and then click **Add**.
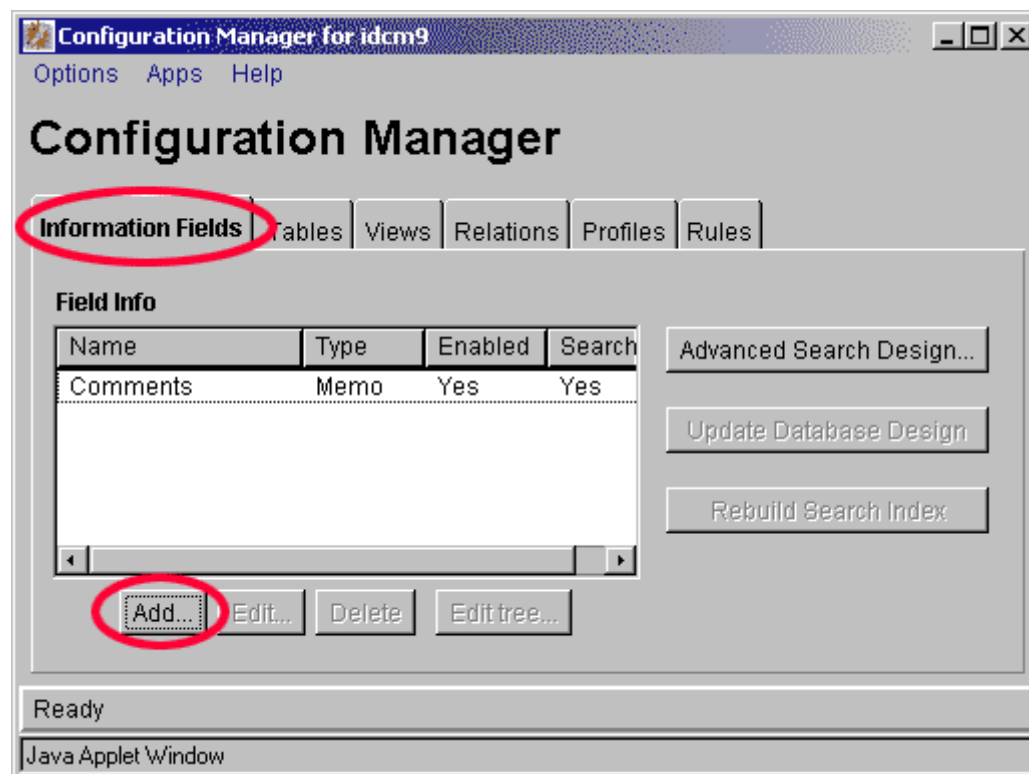
3. The **Add Custom Info Field** screen is displayed.

4. Type **Project** in the Field Name field and click **OK**.
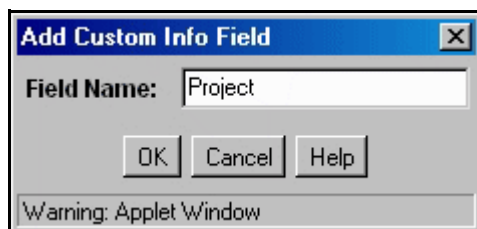
5. The Add Custom Info Field *'Field Name'* screen is displayed.

> **Note:** The field name defines the field in Content Server data tables. The field caption appears on the user interface. By default, the text you enter for the field name will be displayed in the **Field Caption** field on the Add Custom Info Field '*Field Name'* screen. You can change the field caption without affecting the field name. The field caption can contain spaces, the field name cannot.

6. Select **Text** from the **Field Type** choice list.

7. Enable **Option List** and click **OK**. An alert is displayed.

8. If you enable the Option List feature, then you must specify at least one option choice.

9. Click **OK** to close the alert.

10. Click **Configure** next to the **Enable Option List** field. The Configure Option List screen is displayed.

11. Click **Edit** next to the Use option list field and leave all other fields set to the default values.The Option List screen is displayed.

12. Enter **None, A**, **B**, and **C** in the Option List field. Press **Enter** on your keyboard between each option so they populate the choice list as separate options.

> **Tech Tip:** On the Content Check In Form, the choice list will display the options listed in the Default Value field. If there is no default value, the first value listed in the Option List is displayed. To help users avoid inadvertently checking in content with the incorrect value, enter None as the first value. This also will help you, as system administrator, quickly find and correct any content checked in without a value in the custom field.

13. Click **OK** to close the Option List screen, again to close the Configure Options screen, and a third time to close the Add Custom Info Field screen, but do not close the Configuration Manager screen.

# Updating the Database Design and Search Index

The custom metadata field you created is immediately available on the web site, however, the new field must be added to the database design and indexed before it can be used as a search criterion.

1. Click **Update Database Design**.
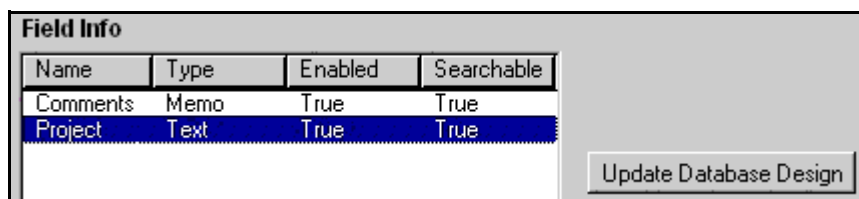
A confirmation screen is displayed.

2. Click **OK**. The field has been added to the database design, but must be added to the index.

3. Click **Rebuild Search Index**.
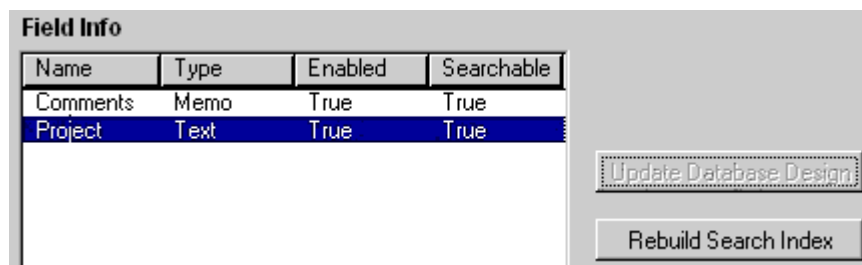
A confirmation screen is displayed.

4. Click **OK**. A confirmation screen is displayed.

5. Click **OK**.

6. Close the Configuration Manager application.

Viewing the New Custom Field
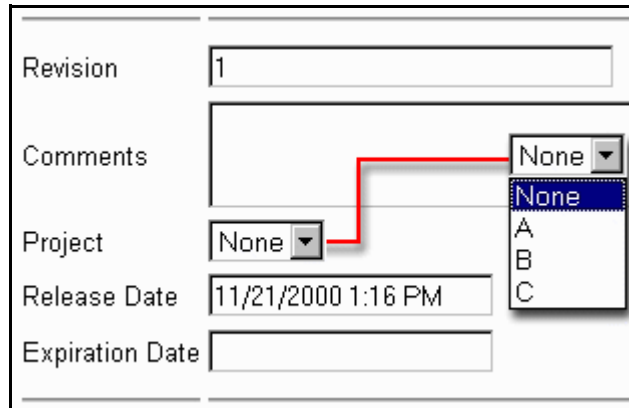
The custom metadata field you created is now available as a checkin field and as a search criterion.

1. Click **New Check In** on the toolbar.

   The Content Check In Form is displayed.

2. Review the Content Check In Form.

   The Project custom field is displayed under the Comments field. The choice list is populated by the project letters you specified.

Tech Tip: All custom fields will be displayed sequentially following the Comments field. You can change the order of the custom fields by changing the field order in the Edit Custom Info Field '*Field Name'* screen.

3. Click **Search** on the toolbar. The Project field is available on the search screen under the Comments field.

THE WEB LAYOUT EDITOR

❖ About the Web Layout Editor (page 5-19)

❖ Links and Pages (page 5-20)

❖ Creating URL Links (page 5-21)

❖ Creating Local Pages (page 5-22)

About the Web Layout Editor

The Web Layout Editor is a Java-enabled tool used to build your Content Server Library Folders hierarchy. Changes made in the Web Layout Editor are automatically reflected in the Library Folders under the My Content Server tray. Knowledge of HTML is helpful, but not required.

4. Click **Web Layout Editor** on the Administration page.

The Web Layout Editor is displayed.

The Web Layout Editor has three sections:

❖ Web Page Hierarchy

❖ Page Properties

❖ Page Links
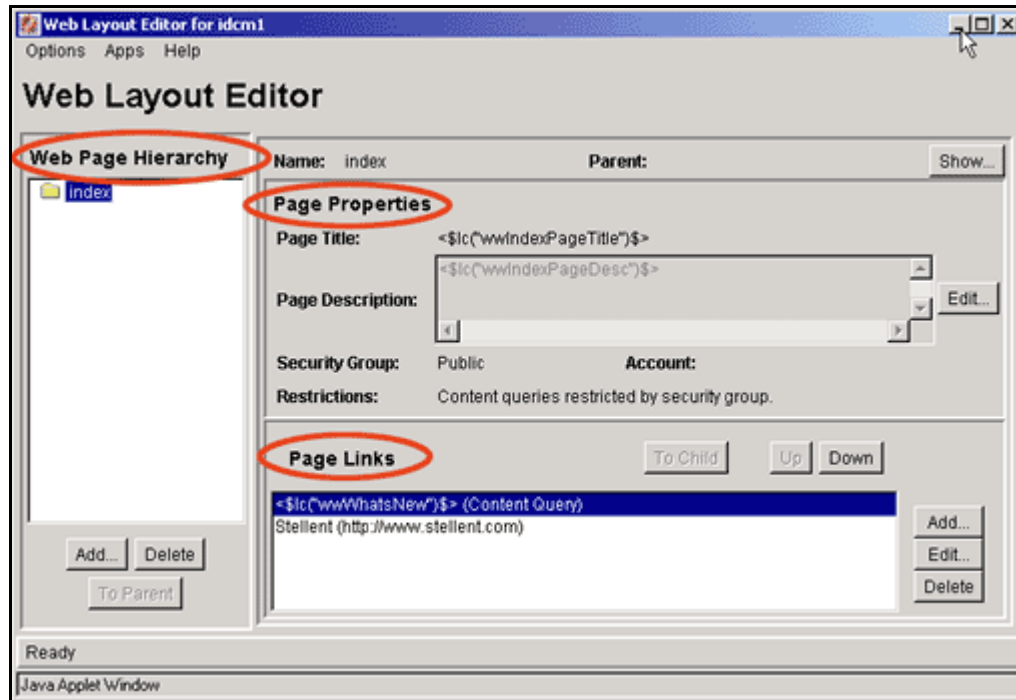
Links and Pages

There are three types of links that can be established on your site:

Link Type	Description
Local Page	A link to a Local Page establishes a link to a page local to your site. A local page can contain links to other local pages, external URLs, and queries.
External URL	A link to an External URL establishes a link to a page external to your site. Internet sites established by business partners, reference sites, and search sites are examples of external URLs.
Query	A Query link initiates a search of the index and returns links to content that matches the criteria of the query. The results can be restricted by security group, account, or both.

You add and modify links and pages using the Page Links section of the Web Layout Editor screen.
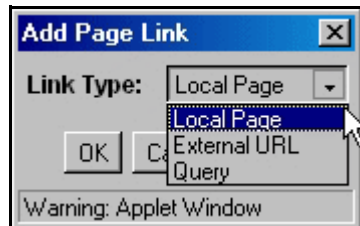
Figure 5-7   Web Layout Editor Screen
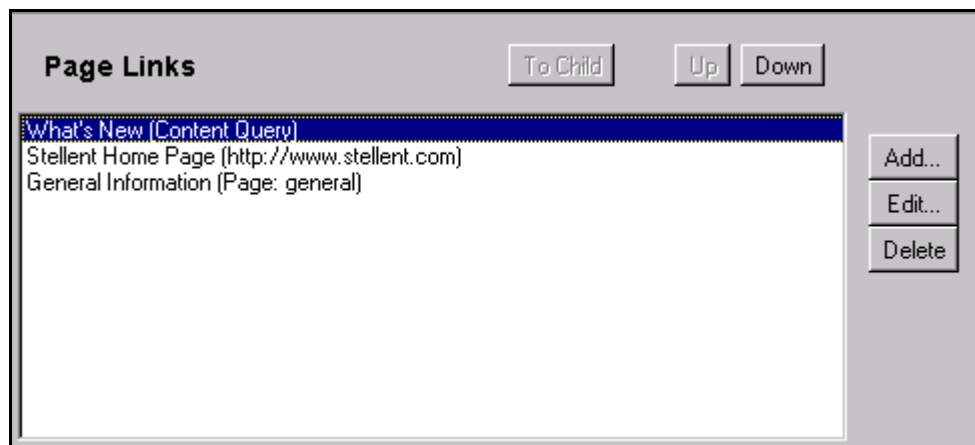
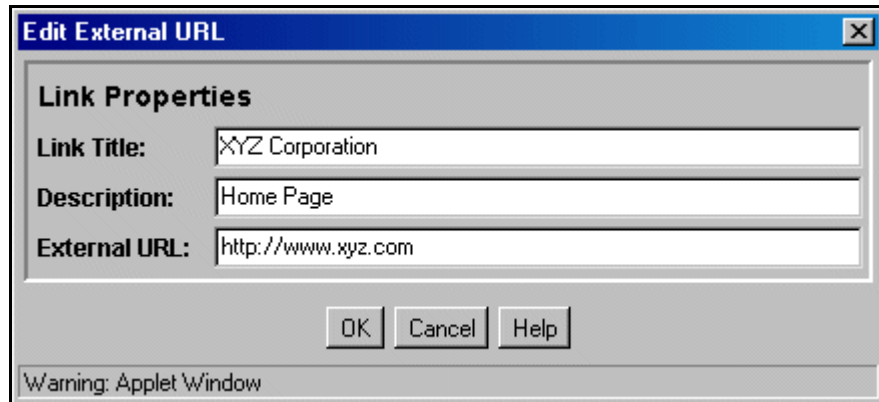
Creating URL Links

To create URL links, complete the following steps:

1. Click the **Add** button in the Page Links section of the Web Layout Editor screen. The Add Page Link screen is displayed.

2. Select **External URL** from the **Link Type** choice list and click **OK**.

    The Edit External URL screen is displayed.

3. Type your company name in the **Link Title** field, **Home Page** in the **Description** field, and the URL of your company's internet web site in the **External URL** field.

4. Click **OK** to close the Edit External URL screen. The URL link is displayed in the Page Links section of the Web Layout Editor screen.

5. Open the Browse Content tray and click Library Query Folders. You should see the link to your company's web site.
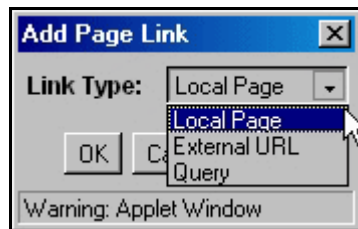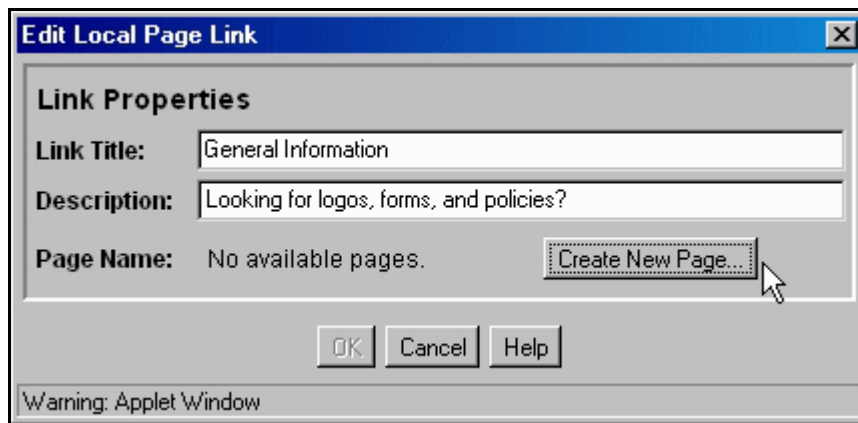

Creating Local Pages

To create local pages, complete the following steps:

1. Click the **Add** button in the Page Link section of the Web Layout Editor screen. The Add Page Link screen is displayed.

2. Select **Local Page** from the **Link Type** choice list, and click **OK**. The Edit Local Page Link screen is displayed.

3. Type **General Information** in the **Link Title** field and **Looking for logos, forms, and policies?** in the **Description** field.

4. Click **Create New Page**. The Add Web Page screen is displayed.

5. Type **general** in the **Page Name** field, **General Company Information** in the **Page Title** field, and **Company Information, Logos, Forms, and Policies** in the **Page Description** field.

6. Select **Directory** in the **Page Type** choice list and **Public** in the **Security Group** choice list.

7. Disable **Restrict content queries by security group** and click **OK**.

8. Click **OK** to close the Edit Local Page Link screen.

The general page is displayed underneath the index page in the Web Page Hierarchy section of the Web Layout Editor screen.

WEB PAGE HIERARCHY

This section covers these topics:

About the Web Page Hierarchy

The Web Page Hierarchy shows the relationship between pages on the Content Server web site.

❖ The index page appears at the top of the Web Page Hierarchy. It is the *parent*, and is displayed as the **Library Query Folders** in the **Browse Content** tray.

❖ The general page you just created is indented and attached to the index page. It is considered a *child* of the index page, and is displayed as a subfolder of the **Library Query Folders** in the **Browse Content** tray.

The link title **General Information** was defined in the **Link Title** field that you filled out in the Edit Local Page Link screen. The description you entered appears under the link on the Library index page.
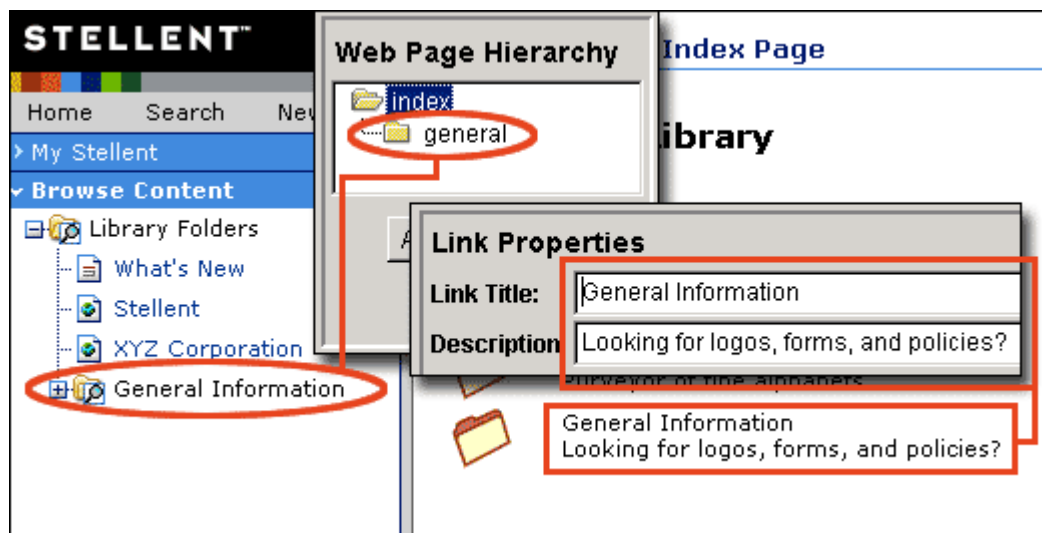
Note: The index page lists predefined queries and is not accessed directly with the default tray layout of Content Server. It is displayed as the **Library Query Folders** in the **Browse Content** tray. To display the index page in the main content area, do the following:

1. Open the **Browse Content** tray, expand **Library Query Folders**, and click **What's New**. A search results page is displayed.

2. Click the folder icon to the left of the **What's New** title. The index page is displayed.

Caution: Do not rename the index page. It is used to define the Library Queries Folders under the Browse Content tray.

Changing the Hierarchy

Clicking **Add** in the Web Page Hierarchy section will also add a local page to the hierarchy, but this approach requires additional steps to arrange the parent/child structure.

First, add three more pages to the web hierarchy.

1. Click **Add** in the Web Page Hierarchy section of the Web Layout Editor.

2. Type **page2** in the **Page Name** and **Page Title** field, and click **OK**.

3. Repeat steps 1 and 2 to add **page3** and **page4** to the web hierarchy.
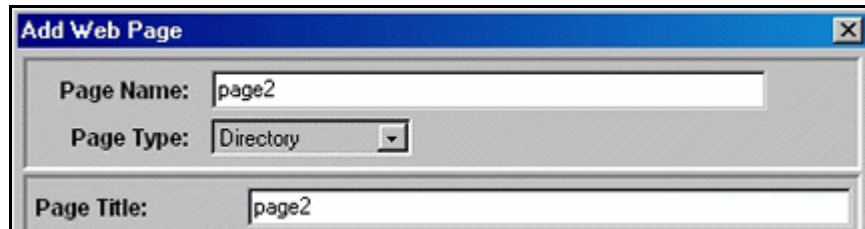
Each page you add in this manner is displayed in the Web Page Hierarchy section at the same level as the index page. To link the pages and establish a parent/child relationship, do the following:

1.   Select **index** in the Web Page Hierarchy section.

2.   Click **Add** in the Page Link section and click **OK** on the Add Page Link screen.

3.   Select **page3** on the **Page Name** choice list, enter **Page 3** in the Link Title and **Page 3 Description** in the Description field, and click **OK**.
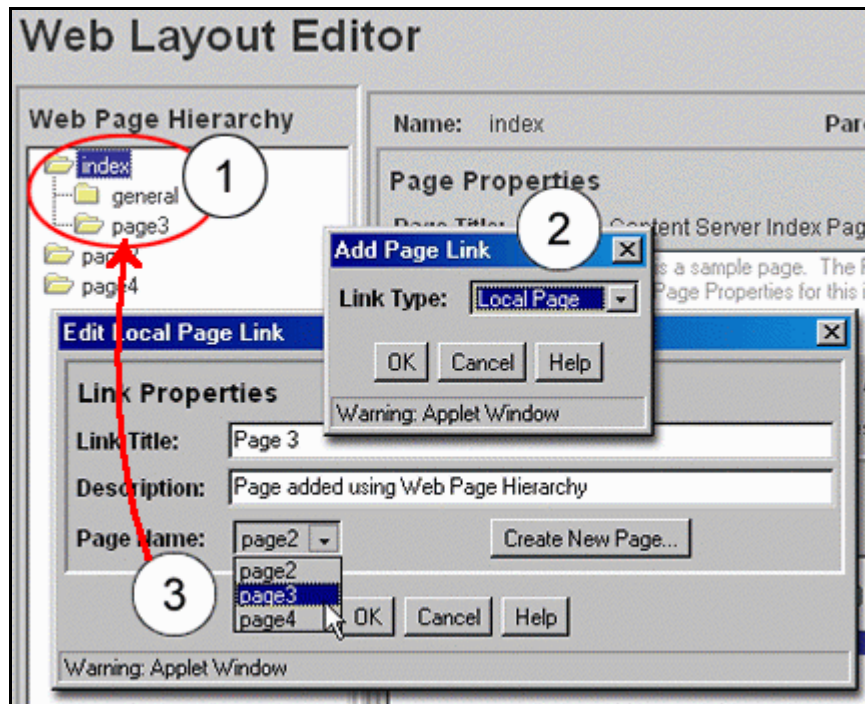
Page3 moves to a child relationship in the Web Page Hierarchy, and a link is established on the index page, appearing as a subfolder of the **Library Query Folders** in the **Browse Content** tray.
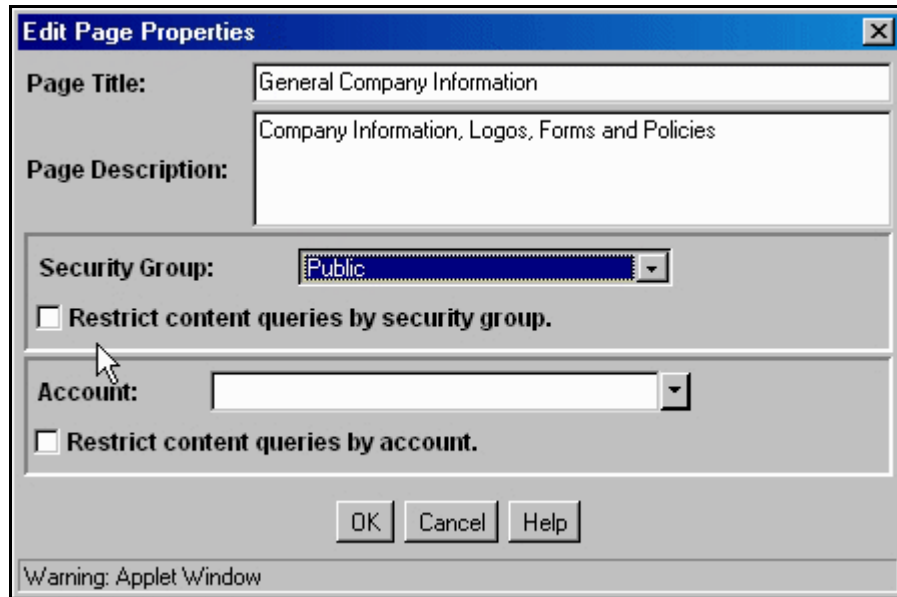
PAGE PROPERTIES

Adding Page Properties

The Page Properties section defines the presentation of a web page.

1. Open the **Browse Content** tray, expand **Library Query Folders**, and click **What's New**.
   A search results page is displayed.

2. Click the folder icon to the left of the **What's New** title. The index page is displayed.

3. Click **General Information**.

   The General Information page is displayed.

4. Select the **general** page in the Web Page Hierarchy section of the Web Layout Editor screen.

   Compare the Page Properties section of the Web Layout Editor screen with the General Information page. The Page Title listed in the page properties is displayed at the top of the browser window and also as the heading of the General Information page.

5. Click **Edit** in the Page Properties section of the Web Layout Editor screen. The Edit Page Properties screen is displayed.

This is the same screen you used to define the page originally, and it can be used to modify the page title and description or to restrict access.

6. Click **Cancel** to close the Edit Page Properties screen.

Adding a Query Link

A query link initiates a search of the index and returns links to content that matches the criteria of the query. The results can be restricted by security group, account, or both.

Query links are created using the Web Layout Editor screen.

1. Select **general** in the Web Page Hierarchy section of the Web Layout Editor screen. The query link will be created on the general page.

2. Click **Add** in the Page Link section of the Web Layout Editor screen. The Add Page Link screen is displayed.
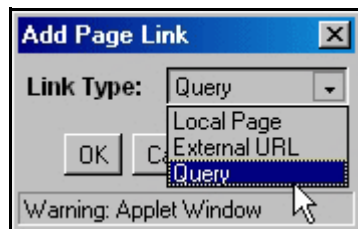
3. Select **Query** from the **Link Type** choice list and click **OK**. The Query Link Definition screen is displayed.

4. Type **Policies** in the **Link Title** field and **Company Policy Statements** in the **Description** field.

5. Select **Type** in the **Field** field, **Matches** in the **Operator** field, and **HRpolicy** in the **Value** field.

6. Click **Add**.

Important: You must click **Add** to include the query expression in the link. Multiple query expressions can be included in one query link by selecting different options and clicking **Add** for each expression to be included.

The query is displayed in the Query Expression field.

7. Click the **Results** tab.

8. Type **Company Policies** in the **Page Title** field.
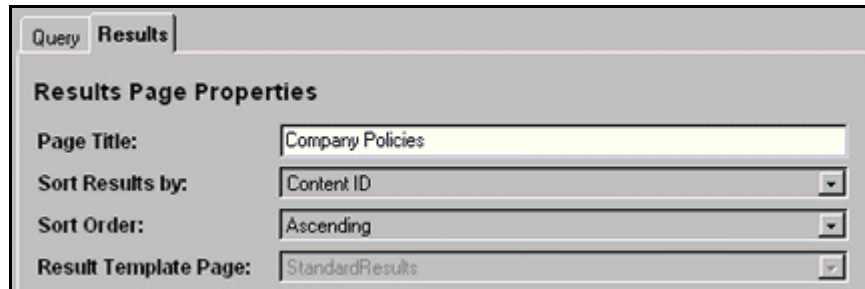
Viewing the Query Results

You have added two links to your web site: a local page and a query. To see the new site:

1. Open the **Browse Content** tray and click **Library Query Folders** and expand the **General Information** folder

2. Click **Policies**. The search index is queried and the results are displayed on the Company Policies page.
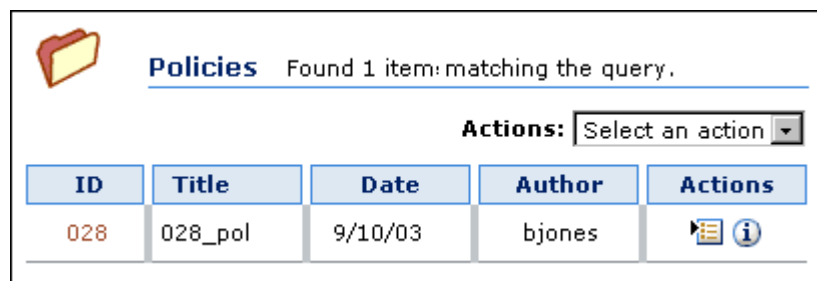
Refining Query Expressions

1. Click the **Query** tab.

2. Select **Author** from the **Field** choice list.

3. Click **Select** next to the **Value** field.

4. Choose **jdoe** as the author and click **OK**.

5. Click **Add**.

The expression is added to the query string.

Important: You must click **Add** to include the query expression in the link.

6. Click **OK**.

View the results of the new query by accessing the Policies link in the General Information subfolder of your Library Query Folders in the Browse Content tray.

1. Open the **Browse Content** tray and expand the **General Information** folder.

2. Click **Policies**.

The search index is queried and the new results are displayed on the Company Policies page. No results were found because there is no content that is the HRpolicy type and authored by Jane Doe.

Customizing the Query Expression

1. Select the **general** page in the Web Page Hierarchy section of the Web Layout Editor screen, then select the **Policies** link in the Page Link section.

2. Click **Edit** in the Page Link section.

    The Query Link Definition screen is displayed.

3. Enable **Custom Query Expression** and select **<AND>** in the query expression text.

    ☑ Custom Query Expression

    ```
    dDocType <matches> `HRpolicy` <AND>
    dDocAuthor <matches> `jdoe`
    ```

4. Type **<OR>** in place of <AND> and click **OK**.

5. View the query results in your browser. All the content that is the HRpolicy type or was authored by Jane Doe is displayed.

    Policies   Found 4 items matching the query.

    Actions: Select an action

ID	Title	Date	Author	Actions
008	008_hr	9/8/03	jdoe	
009	009_hr	9/8/03	jdoe	
010	010_hr	9/8/03	jdoe	
028	028_pol	9/10/03	bjones	

Tech Tip: You can write custom queries and reports using IdocScript and SQL script.

❖ IdocScript is a robust script written just for Content Server software. It is described in detail in the Internet Developer's Kit (IDK), which you can purchase from your reseller.

❖ Your SQL syntax depends on your database. Different databases expect different syntax for items like wildcards and operators. Refer to your database documentation for specific syntax information.

Ordering Page Links

You can rearrange the page links by selecting the one you want to move and clicking **Up** or **Down**. Results of the new location are reflected on the Library page immediately.

1. Select the index page in the Web Page Hierarchy section of the Web Layout Editor screen.

2. Select **General Information (Page: general)** in the Page Links section.

3. Click **Up** to move the link up in the list order.
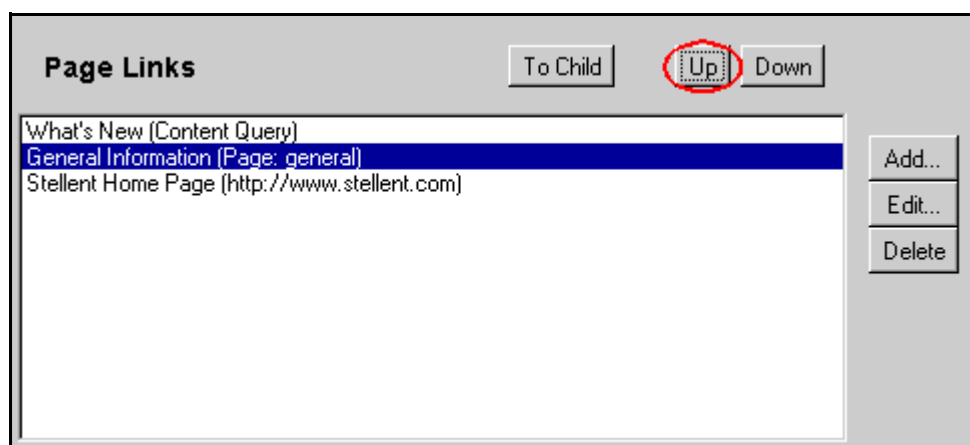
4. Open the **Browse Content** tray and expand the **Library Query Folders** to view the result.
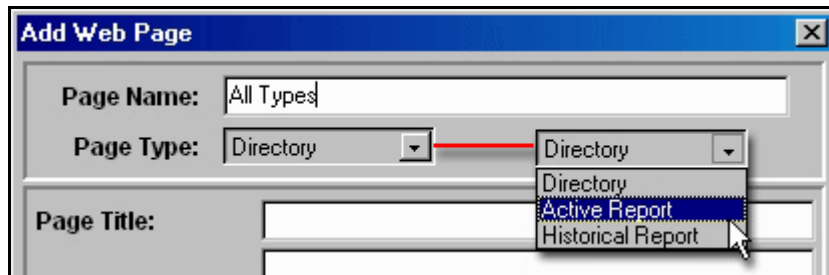
ACTIVE AND HISTORICAL REPORTS

Overview

Reports allow the administrator to create queries about content information and system usage.

Reports are created in the Web Layout Editor screen. The process is similar to creating a local page, but instead of the page type of Directory, you will choose Active Report or Historical Report.

There are two kinds of reports you can create.

Name	Description
Active Reports:	Active reports query the SQL database at the time you view the Web page. Therefore, every time you view the Active Report page, it reflects the most current information in the database. By default, only the first 100 content items that satisfy the query are displayed. A message appears when more than 100 content items satisfy the query. This number can be increased, but response degrades.

Name	Description
Historical Reports:	Historical reports query the SQL database only at the time you create the report. These reports remain static and can be retrieved at a later date. All content items that satisfy the query are included, and multiple-page Historical Reports are formatted with navigation functions for moving from one page to another. You can specify how many rows the report displays before creating the next page.

Because you are querying the SQL database, you must choose the Data Source you want to gather data from. The options are as follows:

Name	Description
Content Types	Content Types lists the Types and their definitions.
User	User lists the defined Content Server users.
Information Fields	Information Fields lists defined items about the custom metadata fields.
Content History	Content History lists actions performed on content.
Workflow Items	Workflow Items lists the defined workflows.
Workflow History	Workflow History lists when the actions—Start, Checkin, Approve, and Reject—were completed and by whom.

# Creating an Active Report

Active Reports query the SQL database at the time you click on the link. We'll create an Active Report that lists all users as shown below.

1. Click **Web Layout Editor** on the Administration page.

2. Select **index** in the Web Page Hierarchy section.

3. Click **Add** in the Page Links section.

4. Select **Local Page** in the Add Page Links screen and click **OK**.

5. Type **All Users** in the **Link Title** field and **All Current Users** in the **Description** field of the Edit Local Page screen.
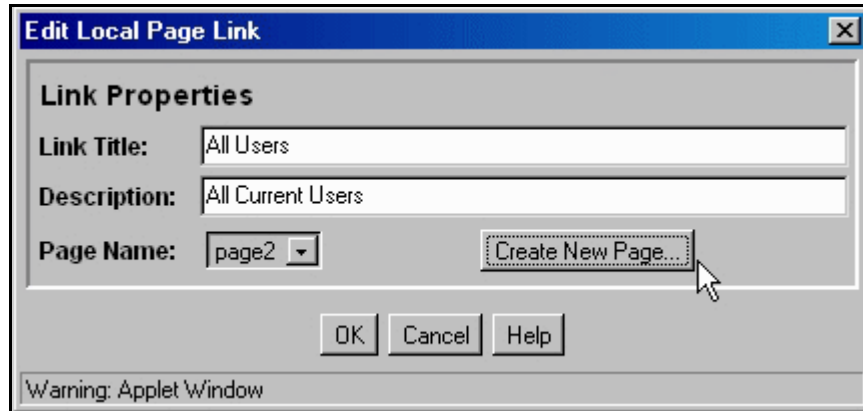
6. Click **Create New Page**.
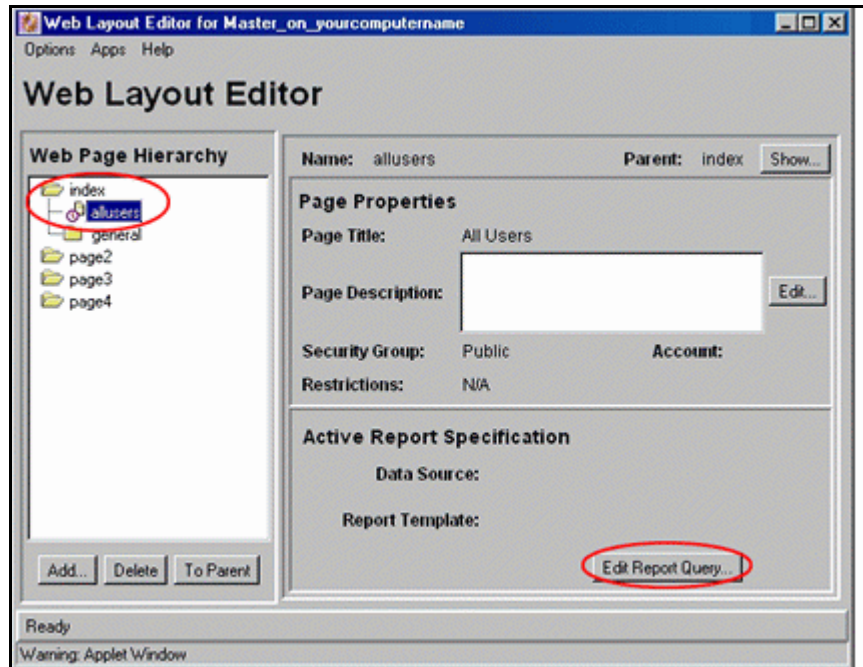
7. Type **allusers** in the **Page Name** field of the Add Web Page screen.

8. Select **Active Report** from the **Page Type** choice list.

9. Click **OK** on the Add Web Page screen and then **OK** on the Edit Local Page Link screen.
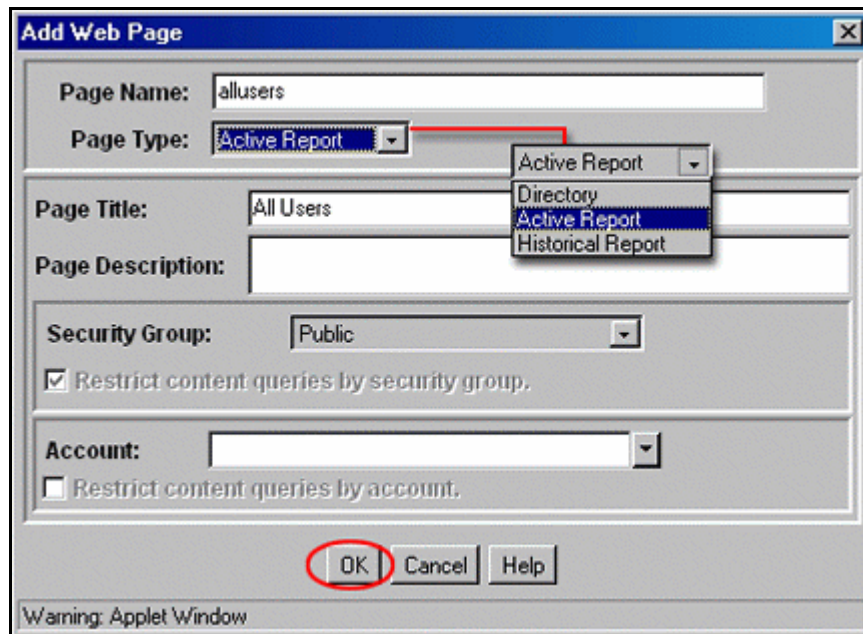
10. Select **allusers** in the Web Page Hierarchy section.

11. Click **Edit Report Query** in the Page Links section to add the report specifications.

12. Select **Users** from the **Data Source** choice list and click **OK**.

13. Close the **Web Layout Editor** applet.

14. View the report by opening the **Browse Content** tray and clicking **All Users**.


Note: You may need to refresh your browser in order for the new link to display.

Creating a Historical Report

Historical Reports query the SQL database at the time the report was created. We'll create a Historical Report that lists all content checked in up to now.

1. Click **Web Layout Editor** on the Administration page.

2. Select **index** in the Web Page Hierarchy section.

3. Click **Add** in the Page Links section.

4. Select **Local Page** in the Add Page Links screen and click **OK**.

5. Type **All Content** in the **Link Title** field and **All Content Checked In** in the **Description** field of the Edit Local Page screen.

6. Click **Create New Page**.

7. Enter **allcheckin** in the **Page Name** field of the Add Web Page screen.

8. Select **Historical Report** from the **Page Type** choice list.
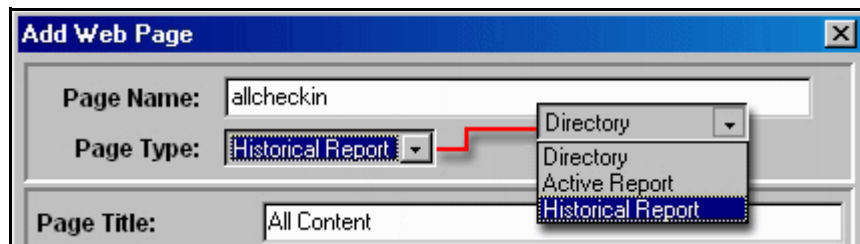
9. Click **OK** on the Add Web Page screen and then **OK** on the Edit Local Page Link screen.

10. Select **allcheckin** in the Web Page Hierarchy section.

11. Click **Create Report Data** in the Historical Report Specification section to add the report specifications.

12. Select **Content History** from the **Data Source** choice list.

13. Select **Action** from the **Field** choice list in the Query Definition section, **Is** from the **Operator** choice list, and **Checkin** from the **Value** choice list.

14. Click **Add**.

15. Click **OK**.

Figure 5-8   Create Historical Report screen

16. Close the **Web Layout Editor** applet.

17. View the report by opening the **Browse Content** tray and clicking **All Content**.

💡 **Note:** You may need to refresh your browser in order for the new link to display.

Refining a Historical Report

You can narrow the report results by adding to the report query. Let's limit the historical report to content checked in after a certain date.

1. Select **allcheckin** in the Web Page Hierarchy section.

2. Click **Create Report Data** in the Historical Report Specification section.

3. Select **Action Date** from the **Field** choice list in the Query Definition section, and **Date Is After** from the **Operator** choice list.

4. Type yesterday's date using the mm/dd/yy format in the **Value** field and click **Add**.
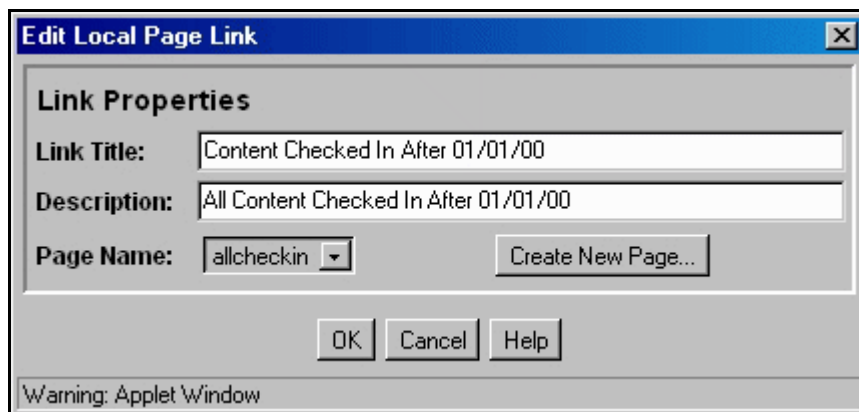

5. Click **OK**.

6. Select **index** in the Web Page Hierarchy section.

7. Select **All Content** in the Page Links section of the Web Layout Editor screen.

8. Click **Edit**.

9. Change the link title to **Content Checked In after '*yesterday's date'*.

10. Change the link description to **All Content Checked In after '*yesterday's date'*** and click **OK**.

11. Close the **Web Layout Editor** applet.

12. View the report by opening the **Browse Content** tray and clicking **Content Checked In after** *'yesterday's date'*.
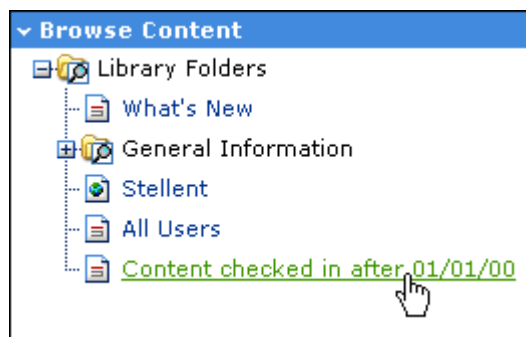
EXERCISE 6: CUSTOMIZING THE LIBRARY FOLDERS

1. Add two local page links to the General Information page, one for **HRforms** and one for **HRresumes**. View the results.

2. Add a query link to the Library page to search for all content authored by Pat Kelly or belonging to the Marketing account. View the result.

3. Add an external URL link to a web site of your choice. Reorder the link so that it is displayed first on the Library page.

4. Delete the Project metadata field and create a new custom field called Marketing Projects. Remember, the field caption can contain spaces, but the field name cannot.

5. Create a new metadata field called Development Projects and have it display above the Marketing Projects field on the Content Check In Form.

6. Create an active report that shows all content belonging to the HRbenefit content type.

You can now proceed with Tutorial 5: Content Profiles (see Chapter 6).

CONTENT PROFILES

OVERVIEW

This section covers these topics:

❖ Creating Content Profiles (page 6-1)

It is recommended that you go through this tutorial from beginning to end, in the suggested order.

CREATING CONTENT PROFILES

You can create content profiles using the Content Manager applet to hide or display metadata on the check in, search, and content information pages based on rules that you define. Content profiles make it easier for users to search for or check in content by refining the metadata options available to them and controlling how metadata fields function.

Once a content profile is created, a links are displayed in the My Check ins and My Searches folders under the My Content Server tray. Clicking the link for the profile displays either a check in or search form showing only the metadata fields defined by the profile.

For a thorough explanation of content profiles, see the Content Server System Administrator's Guide.

This section covers these topics:

❖ Profile Rules (page 6-2)

Profile Rules

To create a content profile, you first need to create a profile rule and then associate the rule to a new profile.

Figure 6-9   Configuration Manager Rules tab
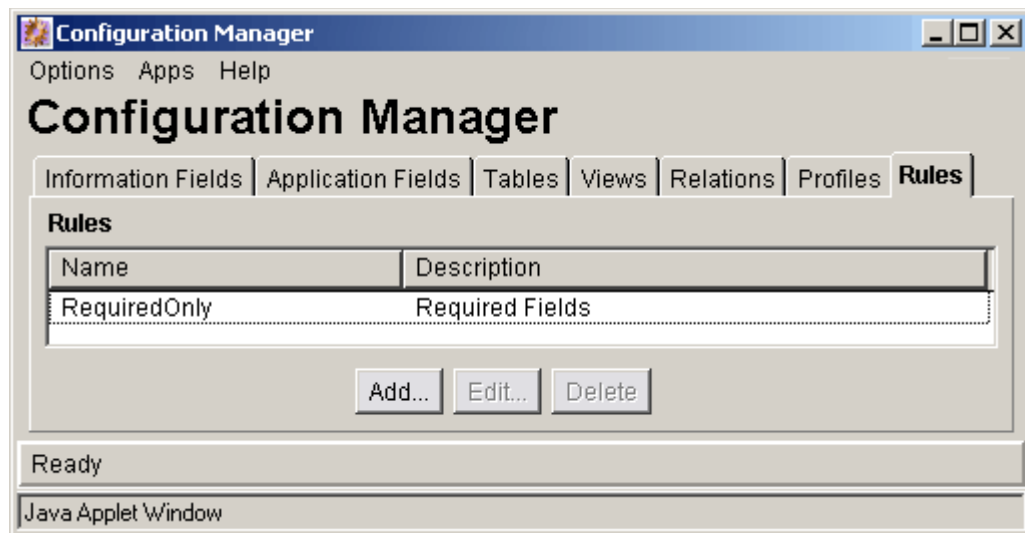
For more information regarding what options are available when creating rules, see the *Managing Repository Content* guide.
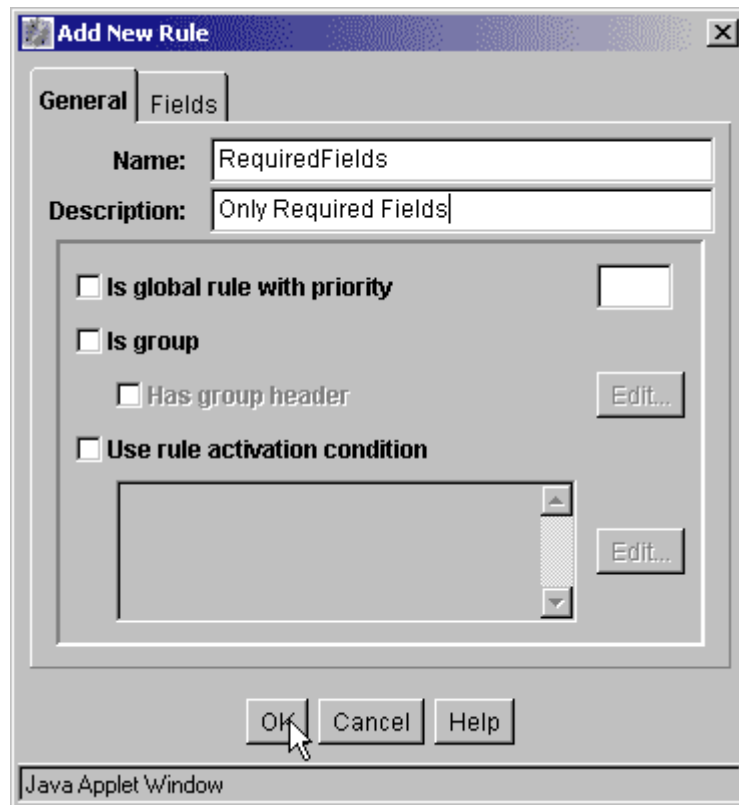
Creating a Profile Rule

Profile rules are created using Rules tab in the Configuration Manager applet.

1. Make sure the Configuration Manager applet is open. If it is not, click **Configuration Manager** on the Administration page.

2. Select the **Rules** tab.

3. Click **Add**. The Add New Rule screen is displayed.

4. Enter **RequiredFields** into the Name field and **Only Required Fields** into the Description field. The rule name cannot contain spaces.

5. Select the **Fields** tab.

6. Click **Add**. The Add Rule Field screen is displayed.
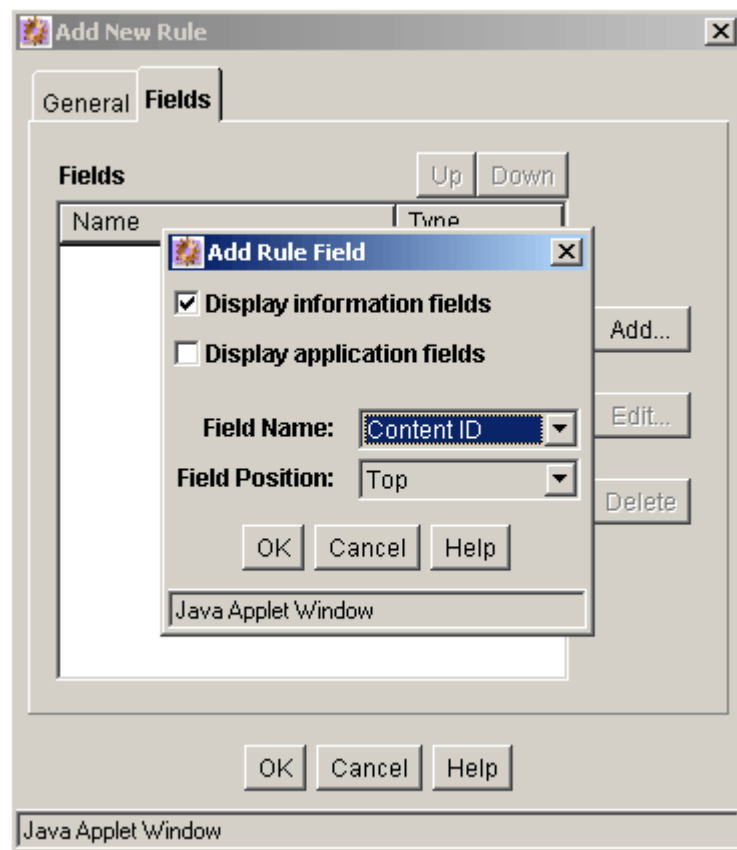
7. Ensure **Display information fields** is enabled and **Display application fields** is disabled.

8. Select **Content ID** from the **Field Name** choice list. Leave the Field Position set to Top.

9. Click **OK**. The Add Rule Field '*fieldname*' screen is displayed.

10. Make sure that **Edit** is selected in the **Type** choice list and click **OK**.

11. Repeat steps 6 through 9 until each of the following fields have been added, maintaining Edit as the default:

- Title (dDocTitle)
- Author (dDocAuthor)
- Type (dDocType)
- Security Group (dSecurityGroup)
- Revision (dRevLabel)

12. Click **OK**, when all of the above fields have been added.

Creating a Content Profile

Content profiles are created using Profiles tab in the Configuration Manager applet.

1. Select the **Profiles** tab.

2. Click **Select** next to the trigger field. The Edit Trigger Field screen is displayed.

3. Select **Security Group** from the **Field Name** choice list and click **OK**.

4. Click **Add** under the Profiles tab. The Add Profile screen is displayed.
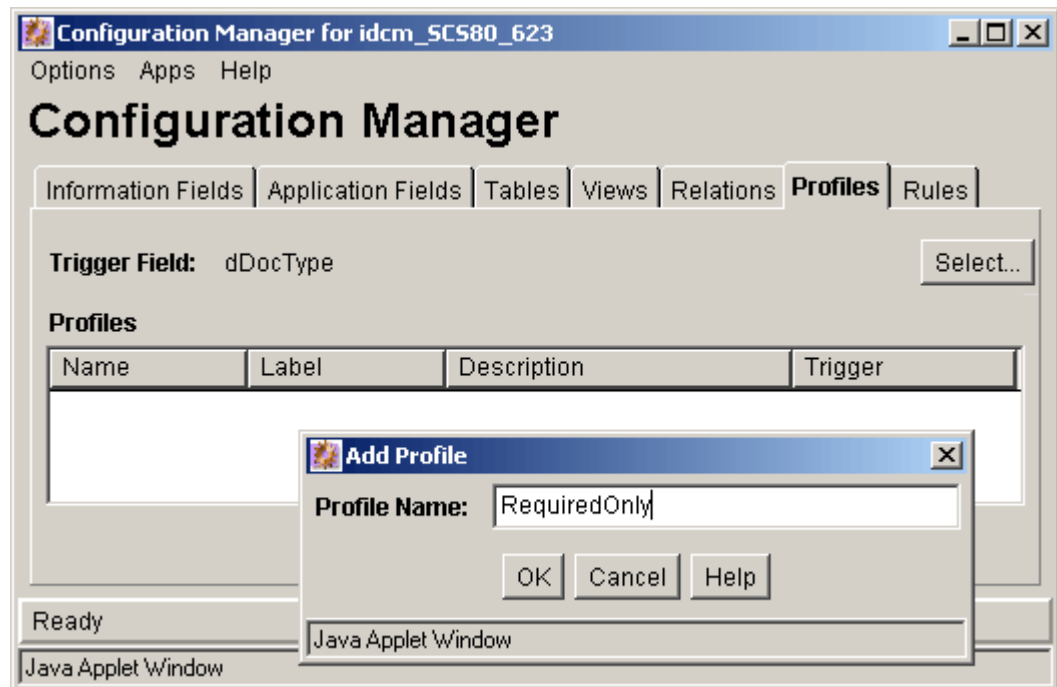
5. Enter **RequiredOnly** into the **Profile Name** field and click **OK**. Profile names cannot contain spaces. The Add Profile '*profile_name*' screen is displayed.

6. Enter **Required Only** in the **Display Label** field. Text entered into the Display Label field can contain spaces, and is displayed as links in the My Check ins and My Searches folders under the My Content Server tray.

7. Enter a description in the **Description** field.

8. Select **Public** from the **Trigger** choice list.

9. Enable the **Exclude non-rule fields** check box.

10. Click **Add** next to the **Rules** field. The Add Rule screen is displayed.
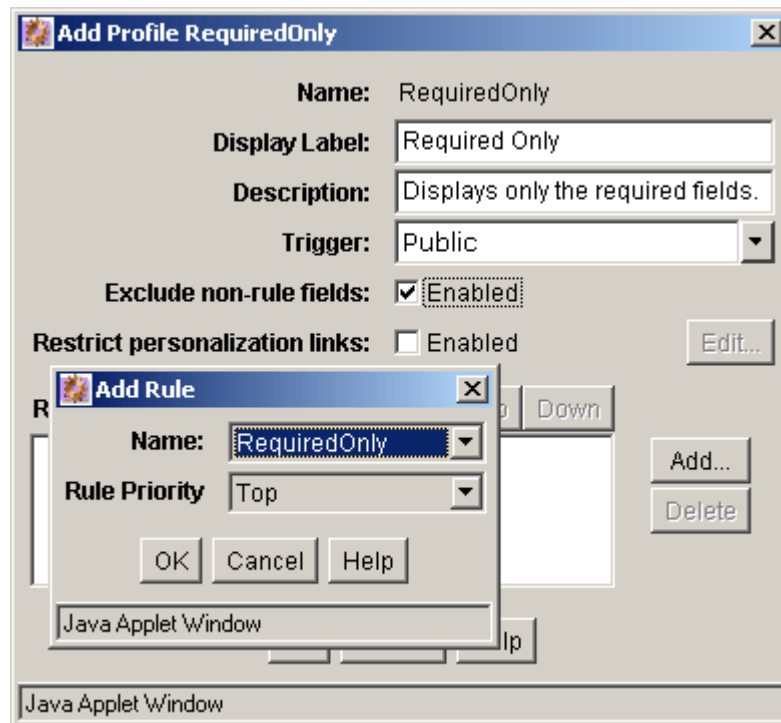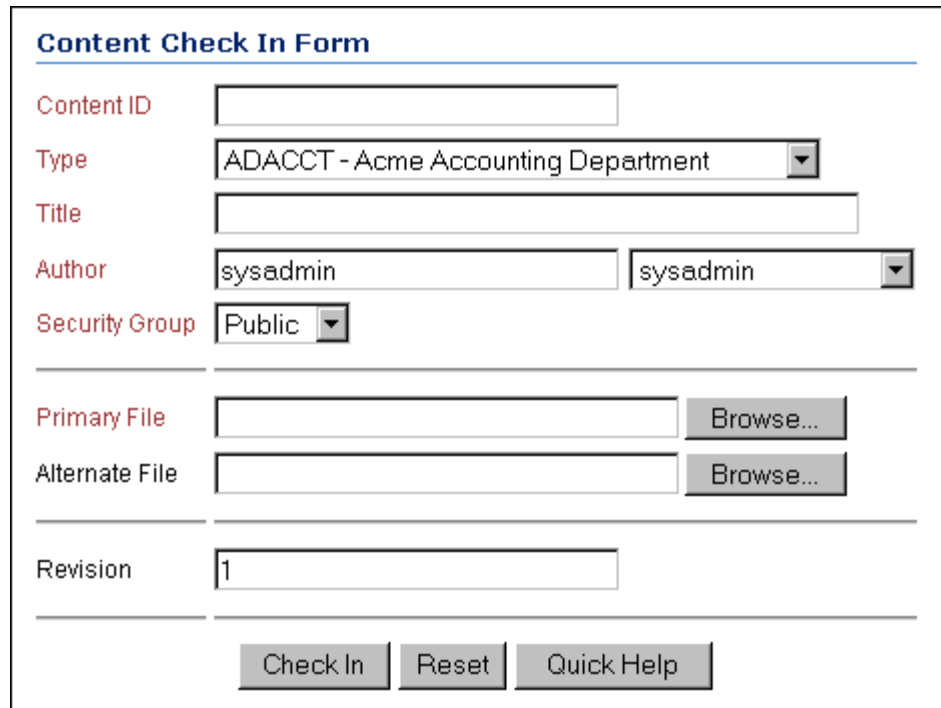
11. Select **RequiredFields** from the **Name** choice list and click **OK**.

12. Click **OK** to accept the new profile. The Add Profile 'profile_name' screen closes.

13. Close the Configuration Manager applet.

Confirming The Content Profile

The content profile you created is immediately available in both the My Check ins and My Searches folders under the My Content Server tray.

1. Click **My Content Server** in the portal to open the tray.

2. Click the icon 📄 next to **My Check ins** to open the folder. The folder expands, showing the new content profile, Required Only.

3. Click **Required Only** in the **My Check ins** folder. The Check in page is displayed. Notice the differences between the profile check in page and the standard check in page.

Figure 6-1   Profile Check In Page

Figure 6-2   Standard Check In Page

You can now proceed with Tutorial 6: The Repository Manager (see Chapter 7).

THE REPOSITORY MANAGER

OVERVIEW

It is recommended that you go through this tutorial from beginning to end, in the suggested order.

The Repository Manager screen is accessed by opening the Administration tray, clicking Admin Applets, and clicking the Repository Manager icon on the Administration page. Open the Repository Manager now.

This section covers these topics:

❖ Working with Content (page 7-2)

❖ Using The Functions Menu (page 7-8)

❖ Working with Subscriptions (page 7-9)

❖ Updating and Rebuilding the Search Index (page 7-19)

WORKING WITH CONTENT

This section covers these topics:

❖

❖

❖

Using the Content Tab
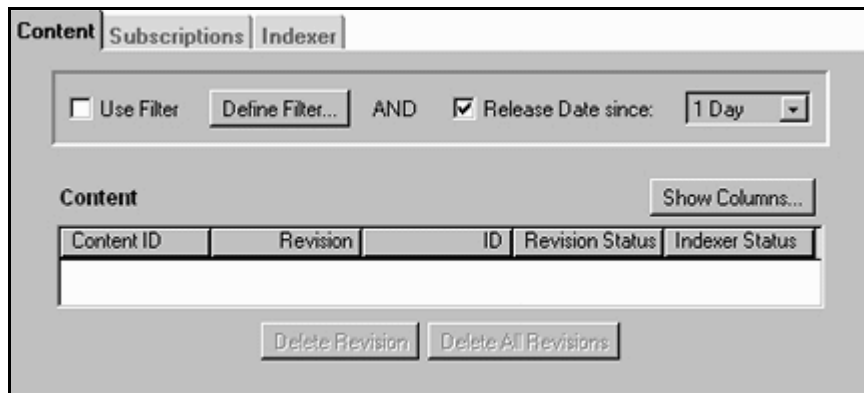
The Content tab displays up to 100 pieces of content that satisfy the specified filter criteria. The default display is all content released in the past day.

From the Content tab, you can perform the same functions you would from the browser:

❖ View status for each content	❖ Resubmit content
❖ View information page for each content	❖ Delete revision
❖ Check out content already in Content Server	❖ Delete all revisions
❖ Undo the check out of content	❖ Add new content into Content Server
❖ Approve or reject content in a workflow	❖ Add a new revision of content into Content Server

Note: The Add New and Add Revision buttons appear on the Repository Manager screen when it is accessed from the Start Menu and run in standalone mode. They are not available when the Repository Manager screen is accessed from the Administration page.

Filtering For Content

You can filter content based on when it was released by enabling **Release Date since** and selecting **1 Day**, **1 Week**, or **4 Weeks** in the choice list.

You can also define your own filter using the following criteria:

Name	Definition
Content ID	Content ID is an open field where you can use wildcards. Wildcards * (one or more characters) and ? (single character) are used for Microsoft Access, and % (one or more characters) and _ (single character) are used for Microsoft SQL Server.
Title	Title is an open field where you can use wildcards as defined above.
Author	Author is an open field where you can use wildcards as defined above.
Type	Type is a dynamic choice list of content types.
Security Group	Security Group is a dynamic choice list of security groups.
Account	Account is a dynamic choice list of accounts.
Checked out	Checked out is a static choice list of Yes and No.
Checked out by	Checked out by is an open field where you can use wildcards as defined above.
Revision Status	Revision Status is a static choice list of Done, Edit, GenWWW Review, Pending, Release, Expired, and Deleted.
Indexer Status	Indexer Status is a static choice list of Index Refinery status.
Conversion Status	Conversion Status is a static choice list of PDF Converter status.

Name	Definition
Indexer Cycle	Indexer Cycle is a static choice list of Index Refinery cycle status.
Publish Type	Publish Type is a static choice list of Content Publisher types.
Publish Status	Publish Status is a static choice list of Content Publisher status.
Latest Revision	Latest Revision displays only the latest revision of content.

Defining Filter Criteria

If you have not already done so, open the Repository Manager screen by clicking Repository Manager on the Administration page.

1. On the Content tab, disable **Release date since** so that all content is displayed.
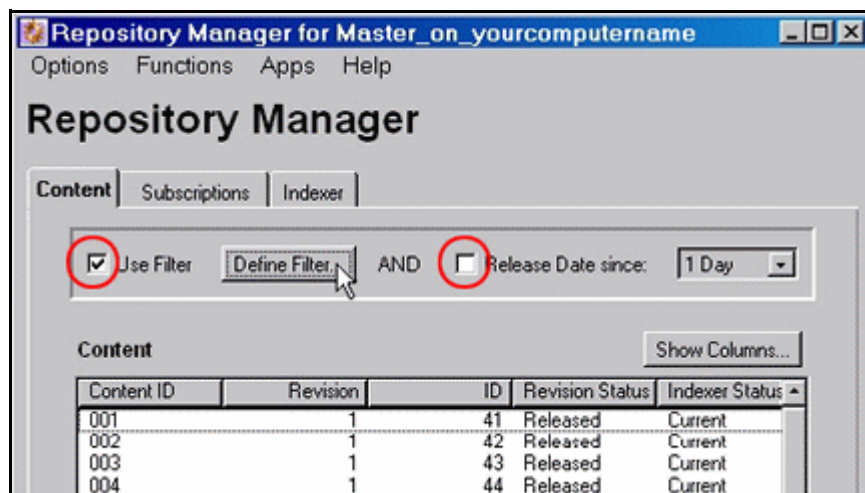
2. Enable **Use Filter** and click **Define Filter**. The Define Filter screen is displayed.

Figure 7-3   Define Filter screen

3. Enable **Content ID** and type ***2** in the field next to it.

⚠️ **Important:** The wildcard used to precede the number 2 is dependant on the database being used with Content Server. The correct wildcard for your database is listed at the bottom of the Define Filter screen as *<wildcard>* = Match Many.

4. Click **OK**. Only content with a 2 in the Content ID field should be displayed.

Displaying Additional Content Info

You can display additional content information in the Repository Manager, including any standard or custom Info Field.
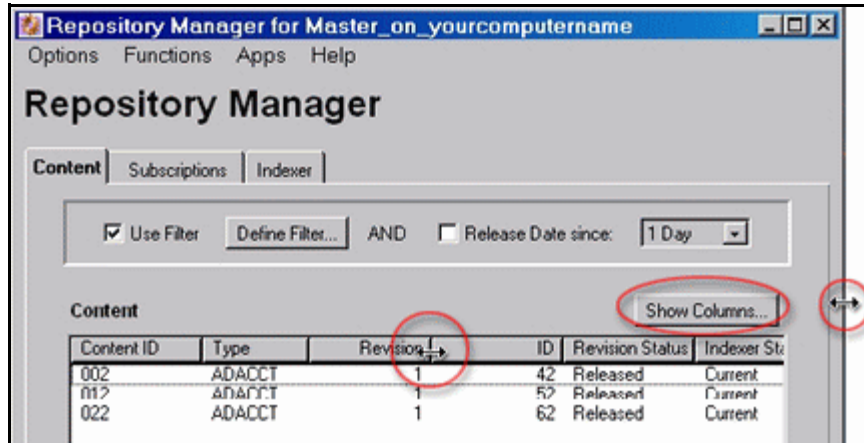
❖ Click **Show Columns** to display the Show Columns screen.

❖ Enable the columns you want to display in the Repository Manager.

❖ If you want to display the same columns each time you open the Repository Manager screen, click **Save Settings**.

❖ Click **OK**.

❖ To adjust the size of the Repository Manager screen, position the cursor on any side or corner of the screen so the double arrow appears, and then drag the screen to the desired size.

❖ To adjust the width of a column, position the cursor on the separator to the right of the column heading so the double arrow appears, and then drag the column to the desired width.
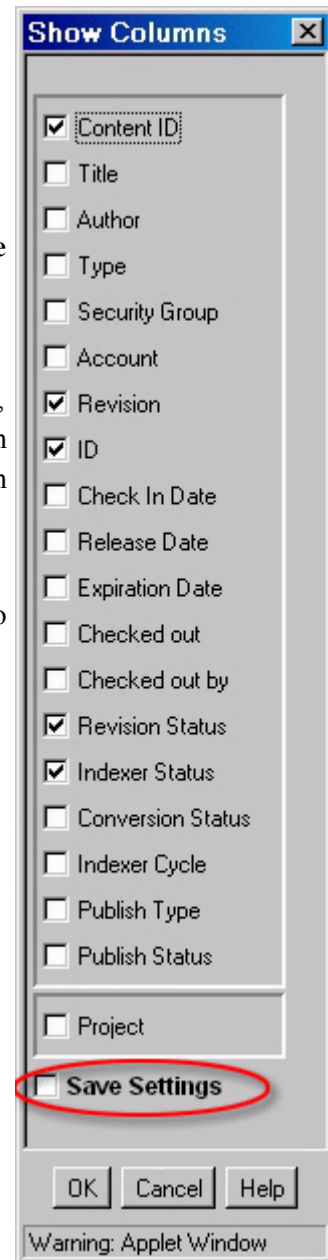
USING THE FUNCTIONS MENU
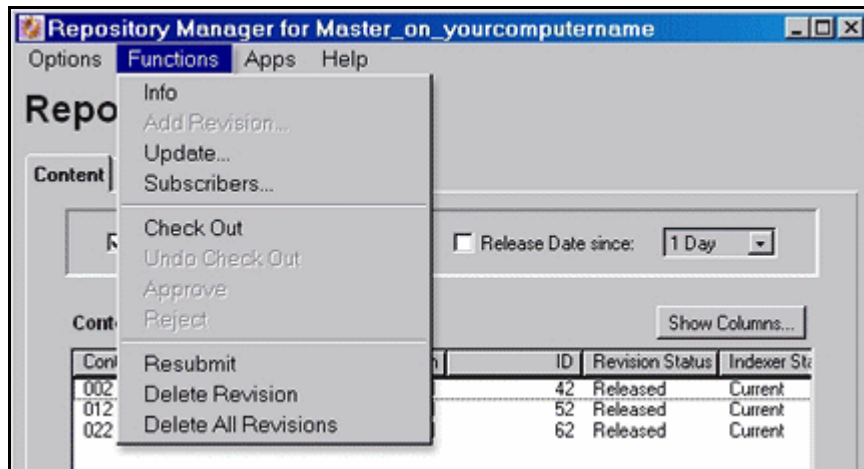
You can make changes to content using the Functions pull-down menu on the Repository Manager screen. In the **Content** field, select the content to which you want to apply a function, then select the function from the Functions pull-down menu.

Tech Tip: If you are on a Windows platform, you can also access the functions menu by right-clicking the content.

Available functions:

Name	Definition
Info	Display information about the file.
Add Revision*	Add a new revision to an existing file.
Update	Change the metadata field values for a file.
Subscribers	View subscriptions and unsubscribe users or aliases.
Check Out	Check out an existing file.
Undo Check Out	Check a file back in with no changes to content or revision number.
Approve and Reject	Approve or reject a file belonging to a workflow.

Name	Definition
Resubmit	Submit a file to the PDF Converter. Normally, resubmit is used only after a file has failed the conversion process. Resubmit is also useful for add-on products, such as Thumbnails and FMBookMan. You cannot resubmit files that are in the PDF Converter queue.
Delete Revision	Delete a revision (same as the **Delete Revision** button at the bottom of the screen).
Delete All Revisions	Delete an entire content item, including revisions (same as the **Delete All Revisions** button at the bottom of the screen).

* Add Revision is available only in a standalone Repository Manager screen accessed from the Start menu.

WORKING WITH SUBSCRIPTIONS

This section covers these topics:

❖ About Subscriptions (page 7-9)

❖ Subscription Types (page 7-10)

❖ Subscribing to a File (page 7-11)

❖ Adding A Criteria Subscription (page 7-12)

❖ Subscribing to a Criteria Subscription (page 7-13)

❖ Assigning a Criteria Subscription (page 7-16)

❖ Viewing Active Subscriptions (page 7-18)

About Subscriptions

Content Server allows all users to manually subscribe to content so that they can be notified by e-mail as soon as the content has been modified and released. This type of subscription is called a file subscription.

The Repository Manager screen allows you, as system administrator, to define content groups to which users can subscribe. This type of subscription is called a criteria subscription.

The Subscriptions tab in the Repository Manager allows you to set the criteria of one or more metadata fields that define a content group. It also enables you to assign users to the subscription. The criteria can be defined by the following fields:

❖ Content ID	❖ Author	❖ Security Group	❖ Account
❖ Title	❖ Type	❖ Revision	❖ Any custom metadata field

Subscription Types

There are two types of subscriptions: basic and criteria.

❖ Users create a basic subscription when they click **Subscribe** on the Content Information page of any file.

❖ You, as system administrator, create criteria subscriptions by defining which metadata field or fields will make up the subscription. The matching content is grouped together in the subscription, enabling users to subscribe to all content matching the defined metadata.

For example, if you set up a criteria subscription with defined metadata of Type, then users have the option of subscribing to a single file or subscribing to all content of the same type.

Note: A file subscription is actually the default criteria subscription, which is called Basic. The defined metadata for the Basic subscription is Content ID. Because the Basic subscription allows a user to subscribe to all content matching the Content ID of the file the user searched for, and the Content ID is a unique identifier, the user can only subscribe to the single file he or she searched for.

Caution: The Basic subscription type can be deleted, but this is not recommended. If you delete the Basic subscription, users will no longer be able to subscribe to single documents.

Subscribing to a File

Perform the following steps to subscribe and unsubscribe to a single content item:

1. Search for content with the Content ID of **030**.

2. Click the **Info** icon . The Content Information page is displayed.

3. Select **Subscribe** from the **Actions** drop-down menu. The menu item changes to Unsubscribe, indicating that you are subscribed.

 Note: You must have an e-mail address entered in your user profile in order for subscription notifications to be sent.

Select **Unsubscribe**. The menu item changes back to Subscribe, indicating that you are not subscribed.
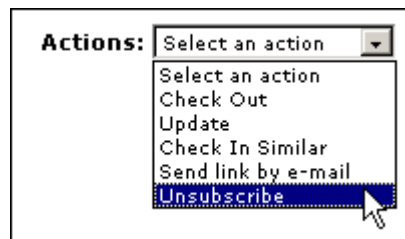
Adding A Criteria Subscription

As system administrator, you can set up a criteria subscription to give users the option of subscribing to a single file or subscribing to all content with the same metadata values.

1. On the Repository Manager screen, click the **Subscriptions** tab. The default subscription, Basic, should be listed.

2. Click **Add**.

    The Add New Subscription Type screen is displayed.

3. Type **TypeSG** in the **Subscription Type** field, **Type and Security Group** in the **Description** field, and enable **Notifications**.

    Enabling **Notifications** causes the system to automatically notify all subscribers if any content in the subscription changes.

4. Click **Fields**.

    The Fields screen is displayed.

5. Enable **Type** and **Security Group** and click **OK**.

6. Click **OK** on the Add New Subscription Type screen.

Subscribing to a Criteria Subscription

Perform the following steps to subscribe and unsubscribe to the new TypeSG subscription.
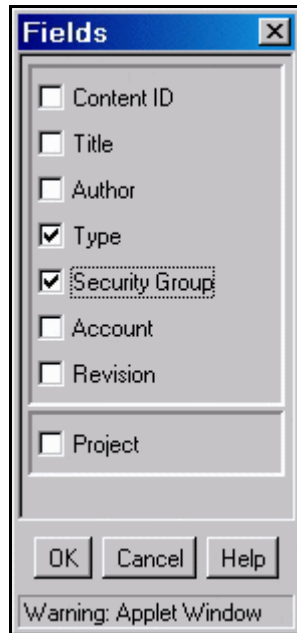
1. Search for content with the Content ID of **030**.

2. Click the **Info** icon ⓘ. The Content Information page is displayed.

    Notice that 030 has a Type of HRresume and a Security Group of Public.

3. Click **Subscribe**. Your subscription options are displayed.

    There are now two ways to subscribe to this content. You can subscribe to the single content item (per the Basic Subscription) or all content with the same Type and Security Group as the 030 file (per the TypeSG Subscription).

Figure 7-4   Subscription Options
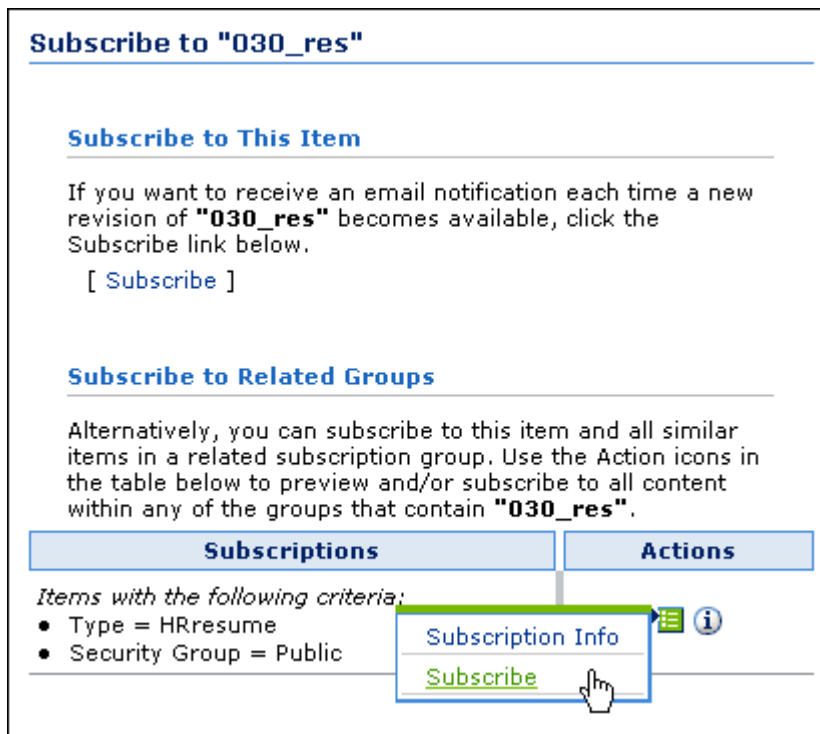
4. Select **Subscribe** from the contextual actions menu   in the Actions column of the Subscribe to Related Groups section.

    The Content Information page is displayed. The **Subscribe** link in the Actions drop-down menu has changed to **Unsubscribe**, indicating that you are subscribed.

5. Select **Unsubscribe** from the Actions drop-down menu.
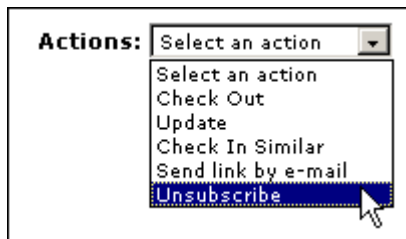
6. Click **Unsubscribe**. The Unsubscribe page is displayed.

7. Click the **Actions** icon to open the contextual menu. Notice that you could unsubscribe from the group by selecting Unsubscribe.

8. Select **Subscription Info** from the contextual menu. The Subscription Info page is displayed. Notice the options you have under the Actions icon contextual menu, and the breadcrumb navigation trail at the top of the page.

9. Click **Unsubscribe** next to the **Action** field to unsubscribe from the group.

Assigning a Criteria Subscription

The system administrator can assign criteria subscriptions to users or groups of users, either directly or by setting up an alias for a group.

If the administrator sets up a subscriptions with specific users, the users can unsubscribe. When using an alias, the users cannot unsubscribe. Only the administrator can remove users from an alias assigned to a subscription.

To assign a subscription to a user, do the following:

1. Click **Repository Manager** on the Administration page to open the Repository Manager screen.

2. Click the Subscriptions tab and select **TypeSG**.

3. Click **Subscribers**. The User subscribed by '*subscription'* screen is displayed.
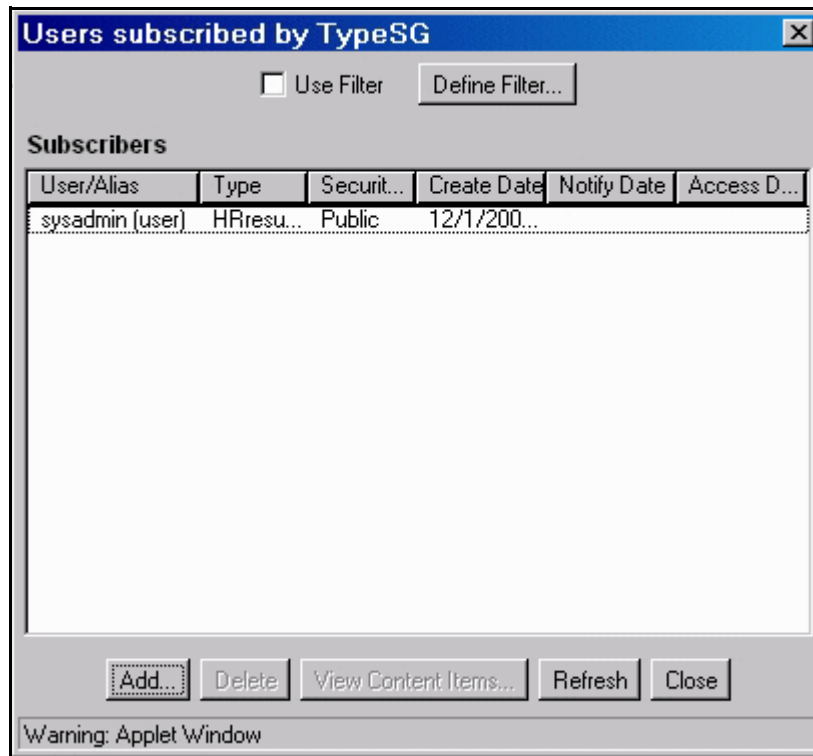
4. Click **Add**. The Add Subscription screen is displayed.
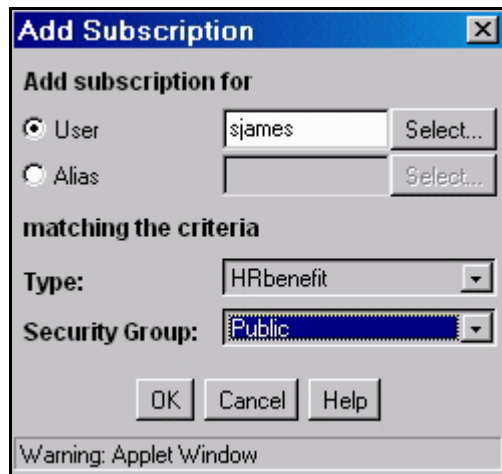
5.   Enable **User** and click **Select.**

     The User screen is displayed.

6.   Select **sjames** and click **OK**.

7.   Select **HRbenefit** from the **Type** choice list and **Public** from the **Security Group** choice list and click **OK**.

8.   Click **View Content Items** to verify your criteria.
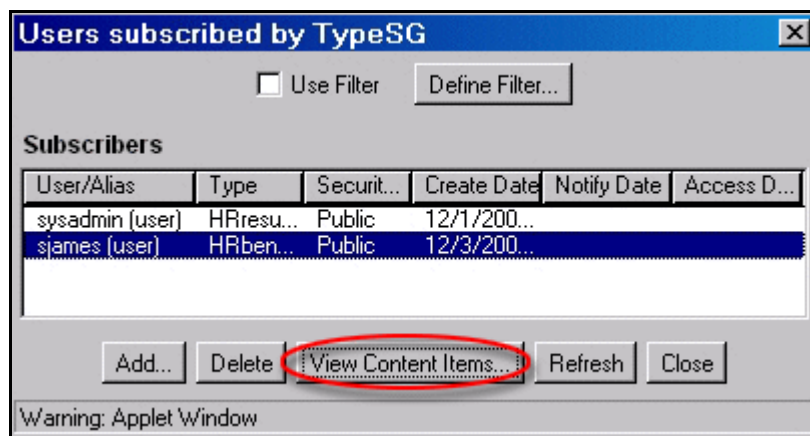
The Content Item Subscribed screen is displayed. All content matching the defined criteria is listed here.
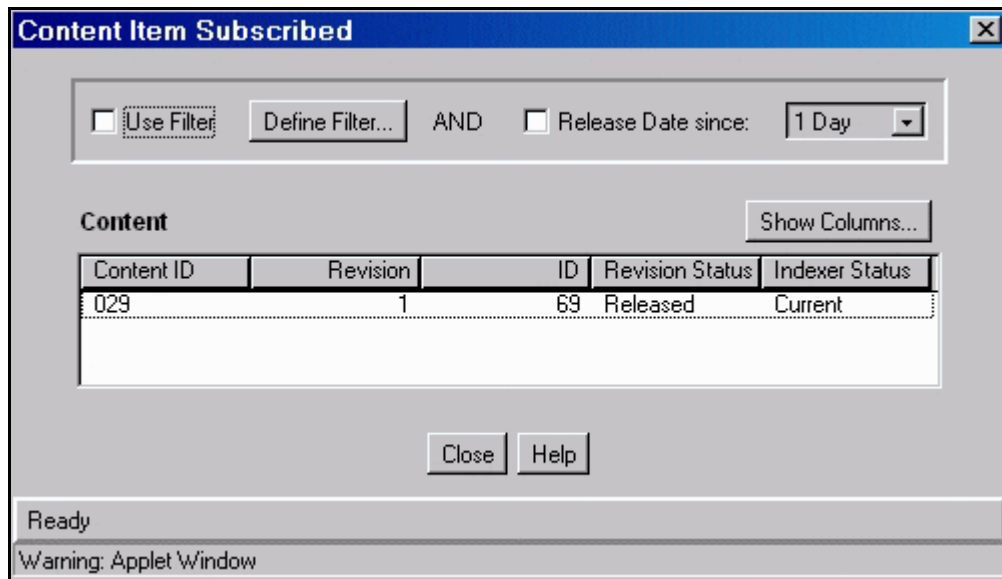
Viewing Active Subscriptions

A user can view the content to which they are subscribed by clicking My Subscriptions under the My Content Server tray.

1. Open a new browser instance and login as Shawn James (username = **sjames**, password = **idc**).

2. Open the **My Content Server** tray.

3. Click **My Subscriptions**. A listing of all subscriptions for Shawn James is displayed.

UPDATING AND REBUILDING THE SEARCH INDEX

This section covers these topics:

Working with the Indexer Tab

The Indexer tab of the Repository Manager screen enables you to update and rebuild the search index. An update and rebuild can occur at the same time.

Automatic Update Cycle

The Automatic Update Cycle updates the search index automatically. You can initiate the update manually by clicking **Start**. The status area provides information on:

Name	Definition
State	Unknown or Finished
Status	idle or active
Start Date	unknown or date/time index started
Finish Date	unknown or date/time index completed
Active Date	not active or date/time is running (reports last status from an active indexing session)

Clicking **Configure** gives you the following options:

Name	Definition
Content Items Per Indexer Batch	The number of items indexed at a time during an automatic update cycle.
Content Items Per Checkpoint	The number of files that will go through all relevant indexing states at a time during an automatic update cycle. In case of a crash, you can restart the index to the checkpoint instead of starting over. Options are 500, 1000, 5000, and 10,000.
Indexer Debug Level	The level of indexer debugging information generated during an automatic update cycle. The higher the debug level, the slower the indexing progresses. The following list shows the debug levels from the least to the most debug information: **none:** No information for each file access is displayed, and no log will be generated. **verbose:** Displays information for each file accessed. Indicates indexed, ignored, or failed, and generates a full report. **debug:** Displays the medium level of information, which is specifically functional. **trace:** Displays the lowest level of information for each activity performed. **all:** Displays the highest level of debug information.
Indexer Auto Updates	Enables or disables automatic index updates. The default is enabled. You may want to disable auto indexing when batch loading content.

Collection Rebuild Cycle
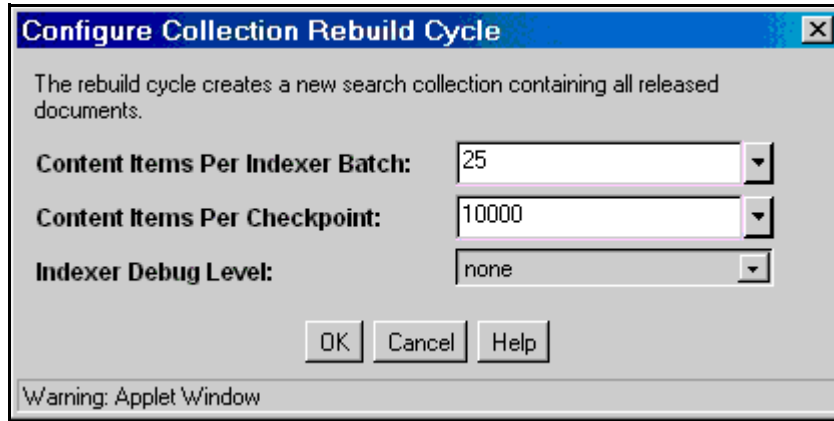
The Collection Rebuild Cycle rebuilds the search index. The status area provides information on the following:

Name	Definition
Total	The total number of content items indexed.
Full Text	The total number of content items that were full-text indexed.
Meta Only	The total number of content items that had only metadata indexed.
Delete	The total number of content items that were deleted out of the index.

Clicking **Configure** gives you the following options:

Name	Definition
Content Items Per Indexer Batch	The number of items indexed at a time during a rebuild.
Content Items Per Checkpoint	The number of files that will go through all relevant indexing states at a time during a rebuild. In case of a crash, you can restart the index to the checkpoint instead of starting over. Options are 500, 1000, 5000, and 10,000.

Name	Definition
Indexer Debug Level	The level of indexer debugging information generated during a rebuild. The higher the debug level, the slower the indexing progresses. The following list shows the debug levels from the least to the most debug information:
	none: No information for each file access is displayed, and no log will be generated.
	verbose: Displays information for each file accessed. Indicates indexed, ignored, or failed, and generates a full report.
	debug: Displays the medium level of information, which is specifically functional.
	trace: Displays the lowest level of information for each activity performed.
	all: Displays the highest level of debug information.

You can now proceed with Tutorial 7: Workflows (see Chapter 8).

WORKFLOWS

OVERVIEW

This section covers these topics:

Note: It is recommended that you go through this tutorial from beginning to end, in the suggested order.

UNDERSTANDING WORKFLOWS

A workflow specifies how content is routed for review and approval before it is released to the system. Users are notified by e-mail when they have a file to review. This section will familiarize you with basic workflow concepts and terminology before you set up the workflows in this tutorial.

This section covers these topics:

Workflow Types

From a workflow administrator's point of view, there are three types of workflows:

❖ In a **Criteria** workflow, a file enters the workflow automatically upon checkin when its metadata matches predefined criteria. In this tutorial, you will create a Criteria workflow to set up a standardized review process for individual documents.

❖ A **Basic** workflow defines the review process for specific content items, and must be initiated manually. In this tutorial, you will create a Basic workflow for a group of related content items.

❖ A **sub-workflow** is a workflow that does not have an initial contribution step. A file can enter a sub-workflow only through a jump from a Criteria workflow. You can find out more information about sub-workflows in the Content Server Help.

Workflow Steps

Each workflow can include multiple review and notification steps, and multiple reviewers can be assigned to approve or reject the file at each step. For each step in a workflow, a set of users and a step type must be defined. The users defined for a step can perform only the tasks allowed for that step type:

Step Type	Description
Contribution	The initial step of a Basic workflow. Contributors are defined when the workflow is created.
Auto-Contribution	The initial step of a Criteria workflow. There are no predefined users involved in this step.
Reviewer	Users can only approve or reject the file; editing is not allowed.
Reviewer/Contributor	Users can edit the file if necessary and then approve or reject it.

Workflow Process

❖ When a file is approved by the minimum number of reviewers for a particular step, it goes to the next step in the workflow.

❖ If any reviewer rejects a file, it goes back to the most recent contribution step for editing.

❖ When a file is approved at the last step in the workflow, the content item is released to the system.

❖ A revision is not released to the system until it exits the workflow. When a file is in a workflow, it can be checked out and checked back in an unlimited number of times without affecting the revision number.

❖ If a Basic workflow contains multiple files, none of them will be released to the system until all of the files have completed the workflow.

❖ The standard workflow process can be customized and made more flexible by using jumps, tokens, and aliases. See the *Using a Workflow* section of the System Administration Guide for more information on these topics.

WORKING WITH CRITERIA WORKFLOWS

This section covers these topics:

❖ Setting Up a Criteria Workflow (page 8-3)

❖ Setting Up Criteria Workflow Steps (page 8-5)

❖ Using a Criteria Workflow (page 8-7)

Setting Up a Criteria Workflow

Suppose that you are Kim Randall, the sub administrator for the Marketing Department. You've been asked to set up a workflow that routes all marketing brochures to the marketing manager (Shawn James) for editing and then to the marketing team (Tom Adams, Pat Kelly, and you) for approval. The marketing department is very busy, so it's difficult to get all three team members to approve materials right away—you all agree that content will be released after approval from two of the three reviewers.

You'll start by creating the workflow:

1. As the system administrator, define a content type called *MktBrochure*. (If you need review how to do this, see The Configuration Manager (page 5-6).)

2. Open a new browser instance and login as Kim Randall (User Name: **krandall**, password: **idc**).

3. Open the Administration tray and click **Admin Applets**. The Administration page is displayed.

4. Click **Workflow Admin**. The Workflow Admin screen is displayed.

Figure 8-1   Workflow Admin screen
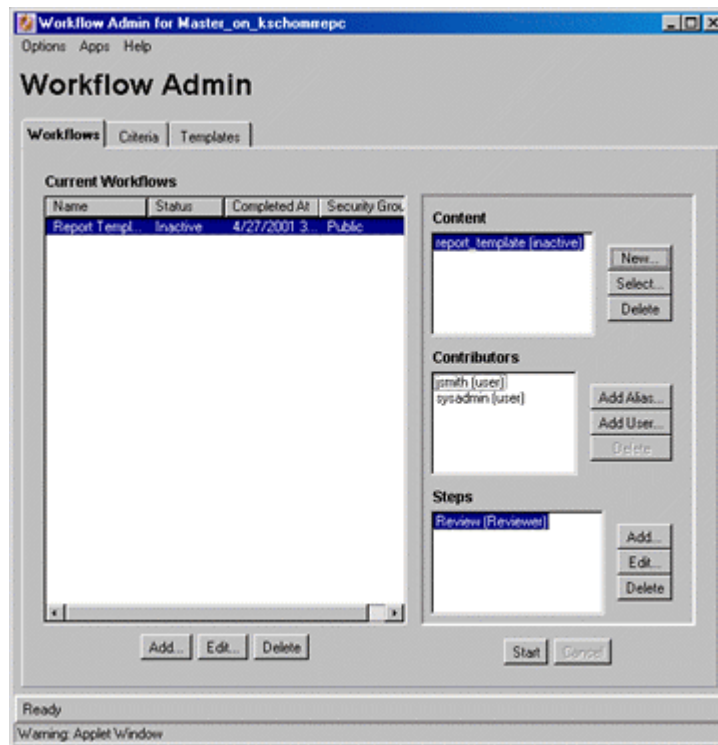
5. Click the **Criteria** tab.

6. Click **Add**. The New Criteria Workflow screen is displayed.

7. Enter *Marketing_Brochures* in the **Workflow Name** field.

Note: A workflow name cannot include spaces.

8. Enter a description in the **Description** field.

9. Select the **Marketing** security group.

10. Enable the **Has Criteria Definition** check box.

11. Select **Type** from the **Field** choice list.

12. Select **MktBrochure** from the **Value** choice list.

13. Click **OK**.

Setting Up Criteria Workflow Steps

Next, you'll add steps to the *Marketing_Brochures* workflow:

1. Click **Add** in the right pane of the Workflow Admin screen. The Add New Step screen is displayed.

Figure 8-2   Add New Step screen

2. Enter *Editor* in the **Name** field.

3. Enter a description in the **Description** field.

4. Enable **Users can review and edit (replace) the current revision**.

5. Click **Add User**. The Add User to Step screen is displayed.

6. Select **sjames** from the list.

7. Click **OK**.

8. Click **OK** on the Add New Step screen.

9. Add a second step called *Marketing_Team* to the workflow. Use the following settings:

    • *Users can review the current revision* enabled

    • *MktTeam* alias

    • Approval required from at least two reviewers (specified under the **Exit Conditions** tab.

    For checked in files to enter the workflow, the workflow needs to be enabled:

10. On the Criteria tab of the Workflow Admin screen, make sure that the *Marketing_Brochures* workflow is selected in the left pane.

Figure 8-3 Criteria Tab of Workflow Admin screen
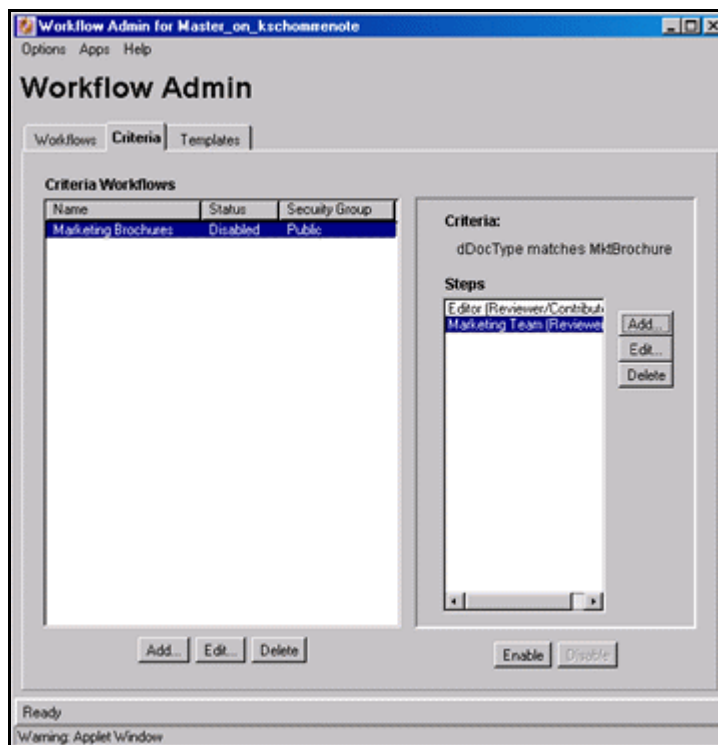
11. Click **Enable**. A confirmation screen is displayed.
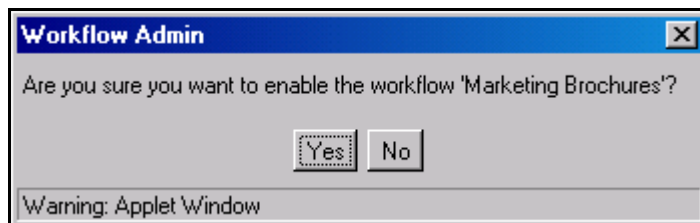
12. Click **Yes** to activate the workflow.

Using a Criteria Workflow

Now that the *Marketing_Brochures* workflow is enabled, any files checked in with the *MktBrochure* type and the *Marketing* security group will enter this workflow.

1. Check in a file from the *Ruggans Tutorial Files/Content* folder using the following metadata:

   • Content ID = 031

   • Type = MktBrochure

- Title = Marketing_Brochure 031

- Author = default

- Security Group = Marketing

- Account = MSP

- Primary File = 031_mkt.doc

If e-mail addresses are set up properly, Shawn James would receive the following e-mail:
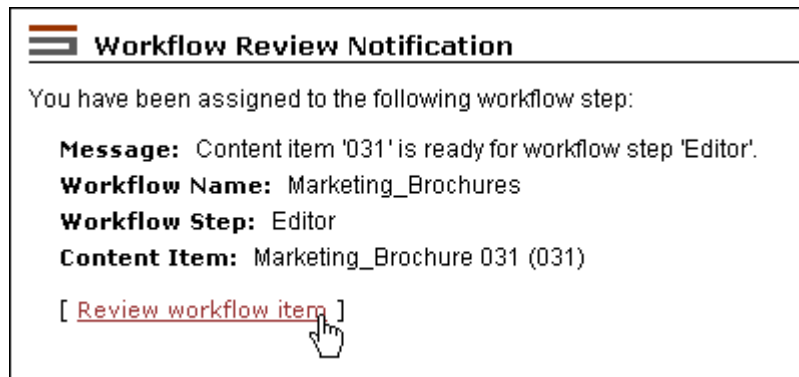
From the e-mail, Shawn James would review the item by clicking the **Review workflow item** link to view the file, information about the revision or the step, or perform one of the tasks conditionally available to him.
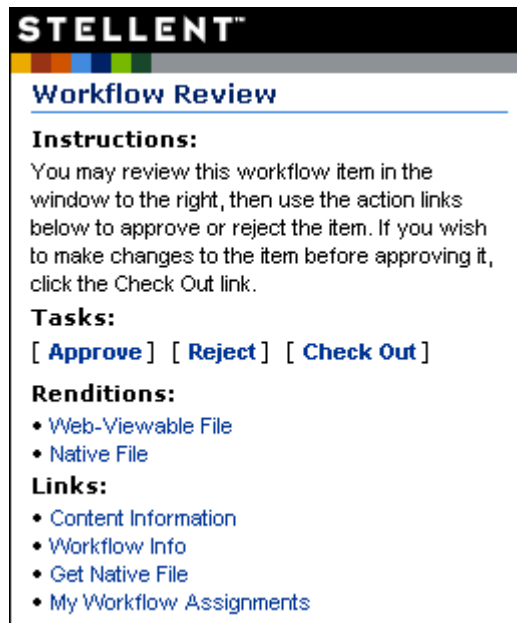
For now, you will access this information from the My Content Server tray.

2. Open a new browser instance and login as Shawn James (User Name: **sjames**, password: **idc**).

3. Open the **My Content Server** tray and click **My Workflow Assignments**.

The Workflow in Queue for sjames page is displayed. From this page, you can click:

- The Content ID link to view the web-viewable file.

- The Action icon   📋   and select one of the following:

  - Workflow Review to open the Workflow Review page.

  - Approve to approve the revision.

  - Reject to reject the revision

  - Content Info to view the Content Information page and check out the content item.

  - Workflow Info to see information about the workflow steps.

  - Workflow Content Items to view a list of all items associated with the workflow.

  - Remove from Queue to remove the workflow from your workflow assignments.

Note: If you remove the workflow from your queue, you can still access the workflow from the Active Workflows page by opening the Content Management tray and clicking Active Workflows.)

- The Info icon to view the Workflow Review page.

As the editor, you want to make a change to the file, so you need to check it out, revise it, and check it back in.

4.   Click the **Info** icon.

The Workflow Review page is displayed.

5.   Click **Check Out**.

The Check Out Confirmation page is displayed. At this point, you could get a copy of the original file and edit it, or you could check in a different file.

6.   Click **Check In**. The Content Check In Form page is displayed.

7. Select the *031_mkt.doc file in the Ruggans Tutorial Files/Content* folder as the primary file.

8. You are finished editing the file and are ready to approve it, so select the **Approve Revision** check box.

9. Click **Check In**.

    At this point, an e-mail notification would be sent to Kim Randall, Tom Adams, and Pat Kelly. For this step of the workflow, you will access this information from the Active Workflows page, found by clicking the Active Workflows link under the Content Management tray.

10. Close the *sjames* browser instance, open a new browser instance, and login as Pat Kelly (User Name: **pkelly**, password: **idc**).

11. Open the **Content Management** tray and click **Active Workflows**. The Active Workflows page is displayed.

12. Click the **Marketing_Brochures** link. The Content Items for Workflow 'Marketing_Brochures' page is displayed.
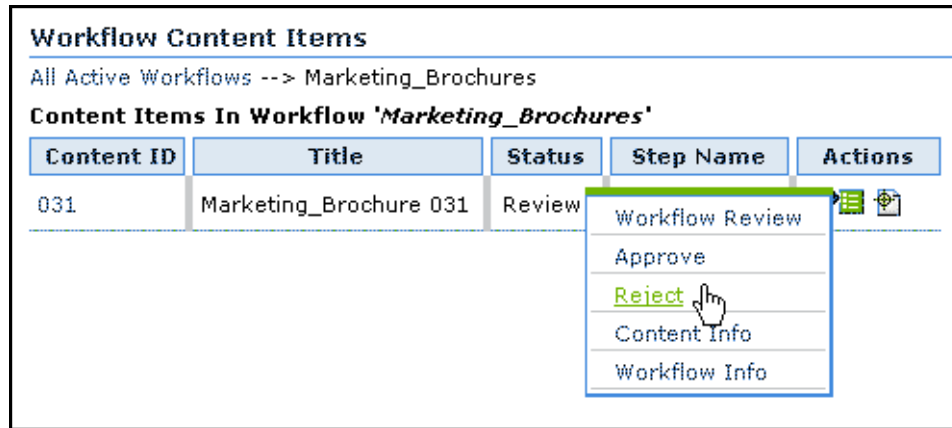
When you clicked the Content ID link and viewed the web-viewable file, you noticed an error in the revision, so you want to reject it.

13. Select **Reject** from the Action icon contextual menu. The Reject Content Item page is displayed.

Figure 8-4   Rejected Content Item page
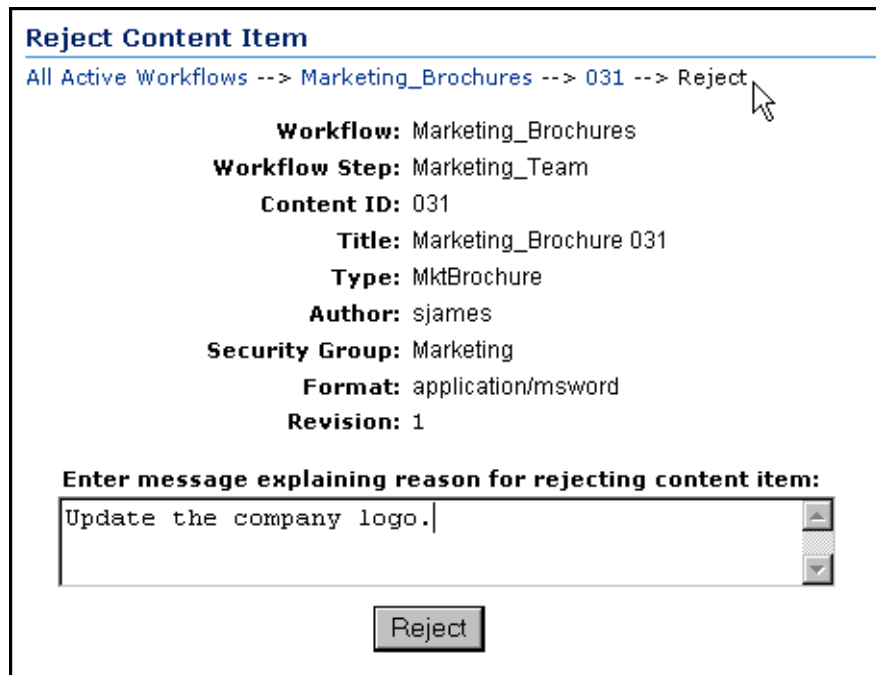
14. Enter a message explaining why you are rejecting the content item.

15. Click **Reject**.

The workflow now returns to the most recent workflow step that permitted contribution, which was the *Editor* step. Shawn James will receive the reject notice, edit the file as necessary, and approve it. The Marketing team will be notified when the revision is ready for approval again.

16. As Pat Kelly, approve the revision.

17. Close the *pkelly* browser instance, open a new browser instance, and login as Tom Adams (User Name: **tadams**, password: **idc**).

18. Approve the revision.

19. Perform a search for the content item, and view the Content Information page.

    Note that the revision was released after the two approvals were made rather than immediately after the file was checked in. Also note that the revision number is 1, even though the file had been checked out and back in.

WORKING WITH BASIC WORKFLOWS

This section covers these topics:

❖ Setting Up a Basic Workflow (page 8-13)

❖ Setting Up Basic Workflow Steps (page 8-14)

❖ Using a Basic Workflow (page 8-17)

Setting Up a Basic Workflow

Shawn James has created two brochure templates that everyone in the Marketing Department needs to review and approve. Kim Randall, the sub administrator for the Marketing department, has been asked to set up a workflow for this purpose. Because there is more than one document and this is a one-time request, she decides to create a Basic workflow.

You, as Kim Randall, will start by creating the workflow:

1. Open a new browser instance and login as Kim Randall (User Name: **krandall**, password: **idc**).

2. Open the Administration tray and click **Admin Applets**. The Administration page is displayed.

3. Click **Workflow Admin**. The Workflow Admin screen is displayed.

4. Click **Add** in the left pane of the Workflows tab. The Add New Workflow screen is displayed.

5. Enter *Brochure_Templates* in the **Workflow Name** field.

6. Enter a description in the **Description** field.

7. Select the **Marketing** security group.

8. Click **OK**.

Setting Up Basic Workflow Steps

Next, you'll add steps to the *Brochure_Templates* workflow:

One of the brochure templates, *025_mkt.doc*, has already been checked in, but now needs to go through the approval process.

1. Click **Select** next to the Content pane. The Add Content to Workflow screen is displayed.
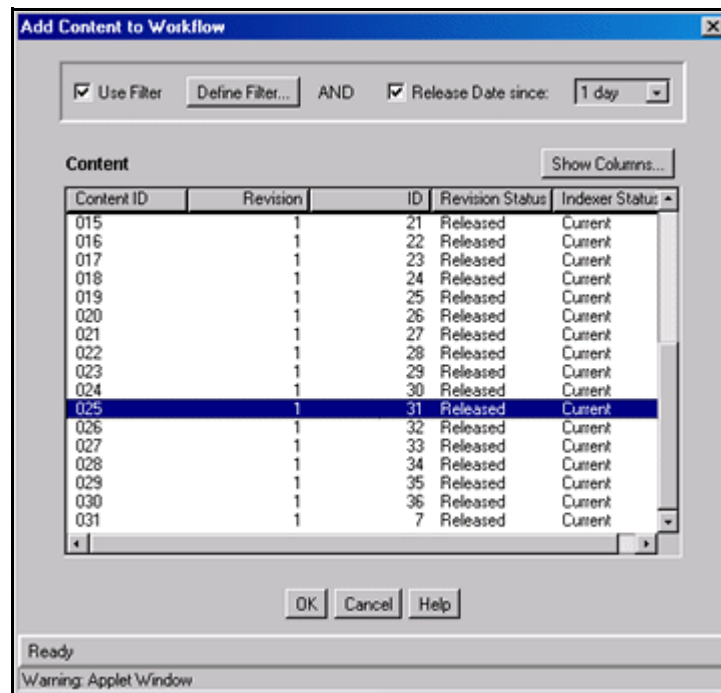
2. Select the **025** content item and click **OK**. The other brochure template has not been checked in yet.

3. Click **New** next to the Content pane. The Add Content to Workflow screen is displayed.
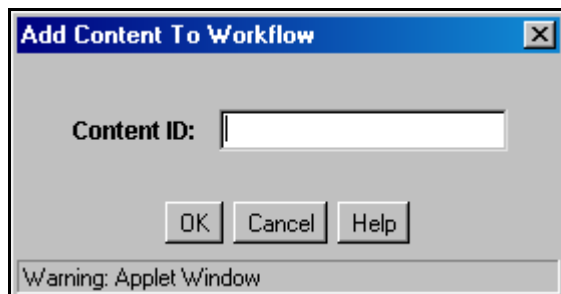
4. Enter **032** as the Content ID for the new content item and click **OK**. Shawn James will check in the files for the initial contribution step.

5. Click **Add User** next to the Contributors pane. The Add User to Step screen is displayed.

6. Select **sjames** from the user list and click **OK**. Only one review step is required for this workflow.

7. Click **Add** next to the Steps pane. The Add New Step screen is displayed.

Figure 8-5   Add New Step screen

8.   Enter *Review* in the **Name** field and a description in the **Description** field.

9.   Enable *Users can review the current revision* so that the reviewers are unable to edit the files.

10. Click **Add User**. The Add User to Step screen is displayed.

11. Select Pat Kelly, Tom Adams, and Kim Randall as the reviewers. Holding down the Ctrl key enables you to select multiple users.

12. Click **OK**.

13. You want everyone to approve the content items, so click the **Exit Conditions** tab and select **All reviewers**.

14. Click **OK**.

15. Make sure that the workflow is selected in the left pane of the Workflows tab, and click **Start**. The Start Workflow *Brochure_Templates* screen is displayed.
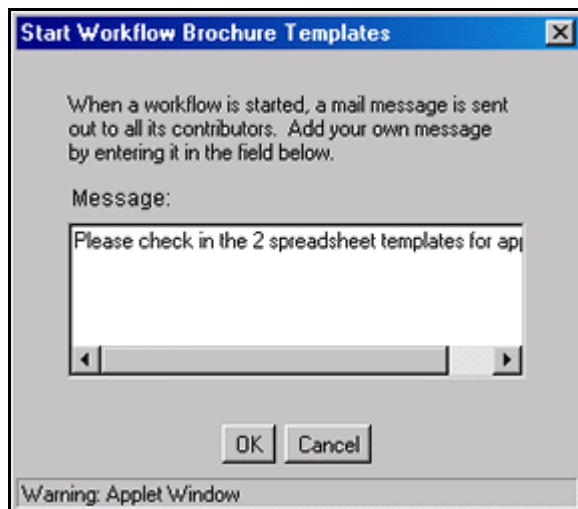
16. Enter a message to be sent to the contributor (Shawn James).

17. Click **OK**.

Using a Basic Workflow

As soon as the *Brochure_Templates* workflow is started, Shawn James receives the following e-mail:
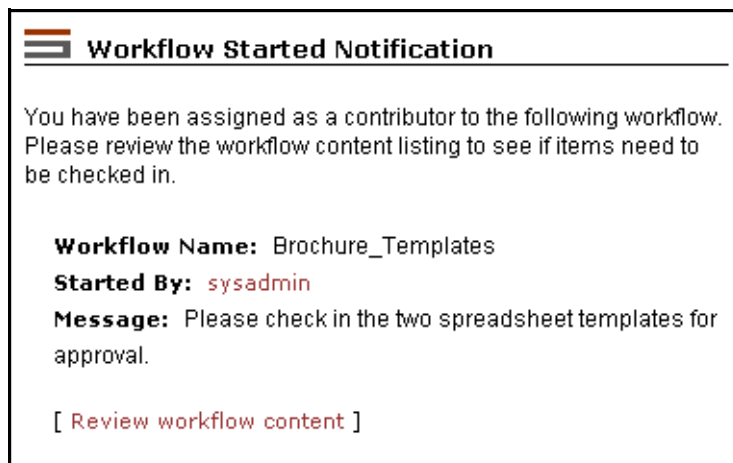
From the e-mail, Shawn James would click the link to review the workflow content. For now, you will access this information from the Active Workflows link under the Content Management tray.

1. Open a new browser instance and login as Shawn James (User Name: **sjames**, password: **idc**).

2. Open the **Content Management** tray and click **Active Workflows**. The Active Workflows page is displayed.

3. Click the **Brochure_Templates** link.

   The Workflow Content Items page is displayed, listing the two content items that were specified for the initial contribution step.

4. Select **Checkout** from the Action icon contextual menu for the 025 content item. The Checkout Confirmation page is displayed.

5. Click **Check In**. The Content Check In Form page is displayed.

6. Select the *025_mkt.doc* file in the *Ruggans Tutorial Files/Content* folder as the primary file, and select Mkt for the **Account** field.

7. Select the **Revision Finished Editing** check box.

> **Note:** The workflow will not move to the next step if the Revision Finished Editing check box is left blank. You would need to check the file out and then back in again.

8. Click **Check In**. The Check In Confirmation page is displayed. At this point, an e-mail notification would be sent to Kim Randall, Sally Wilson, and Pat Kelly.

9. Check in the **032** content item, using the *032_mkt.doc* file in the *Ruggans Tutorial Files/Content* folder as the primary file, and leave the **Account** field blank. Another e-mail notification will be sent to Kim Randall, Tom Adams, and Pat Kelly for this second content item. Note that Shawn James doesn't have any more actions to perform.

10. Close the *sjames* browser instance, open a new browser instance, and login as Pat Kelly (User Name: **pkelly**, password: **idc**).

11. As Pat Kelly, navigate to the Content Items for Workflow 'Brochure_Templates' page.

12. Click the **Review** link for one of the content items. An error message is displayed, telling you that Pat Kelly does not have account privileges for the content item. The content item was checked in with no account, while Pat Kelly only has permission to the *Mkt/A* and *MSP* accounts.

Content Server Request Failed

Unable to retrieve workflow information for '025'. User '(Err)' does not have sufficient privileges to access content without accounts.

> **Important:** It is important to make sure that the users assigned to a workflow have access to both the security group and the account of the content items.

To resolve the situation, you could change Pat Kelly's account access, or you can update the account of the content item. Since the same account issues apply to Tom Adams, you will add the *[documents without accounts]* classification to the *pkelly* and *tadams* user logins.

13. Open a new browser instance and login as the system administrator (User Name: **sysadmin**, password: **idc**).

14. Add the *[documents without accounts]* classification to the *pkelly* and *tadams* user logins. (To review how to do this, see Assigning Accounts to Users (page 4-14).)

15. Return to Pat Kelly's browser instance, and navigate to the Content Items for Workflow 'Brochure_Templates' page.

16. Click the **Review** link for one of the content items.

The Workflow Step Information for 'content ID' page is displayed, indicating that Pat Kelly now has access to content that doesn't have an account.

17. Return to the Content Items for Workflow 'Brochure_Templates' page and approve the two content items.

18. Close the *pkelly* browser instance, open a new instance, and login as Tom Adams (User Name: **tadams**, password: **idc**).

19. Approve both content items.

20. Close the *tadams* browser instance, open a new instance, and login as Kim Randall (User Name: **krandall**, password: **idc**).

21. Approve both content items.

22. Return to the system administrator's browser instance, and perform a search for the two content items.

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 B-1)

❖ W3C® Software Notice and License (page B-2)

❖ Zlib License (page B-3)

❖ General BSD License (page B-4)

❖ General MIT License (page B-5)

❖ Unicode License (page B-5)

❖ Miscellaneous Attributions (page B-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 the documentation associated with the Data File(s) or Software that the data or software has been modified.

THE DATA FILES AND SOFTWARE ARE 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 OF THIRD PARTY RIGHTS. IN NO EVENT SHALL THE COPYRIGHT HOLDER OR HOLDERS INCLUDED IN THIS NOTICE BE LIABLE FOR ANY CLAIM, OR ANY SPECIAL INDIRECT OR CONSEQUENTIAL DAMAGES, OR ANY DAMAGES WHATSOEVER RESULTING FROM LOSS OF USE, DATA OR PROFITS, WHETHER IN AN ACTION OF CONTRACT, NEGLIGENCE OR OTHER TORTIOUS ACTION, ARISING OUT OF OR IN CONNECTION WITH THE USE OR PERFORMANCE OF THE DATA FILES OR SOFTWARE.

Except as contained in this notice, the name of a copyright holder shall not be used in advertising or otherwise to promote the sale, use or other dealings in these Data Files or Software without prior written authorization of the copyright holder.

_____Unicode and the Unicode logo are trademarks of Unicode, Inc., and may be registered in some jurisdictions. All other trademarks and registered trademarks mentioned herein are the property of their respective owners

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.

Portions Copyright © 1990-1998 Handmade Software, Inc. All rights reserved.

Portions Copyright © 1988, 1997 Aladdin Enterprises. All rights reserved.

Portions Copyright © 1997 Soft Horizons. All rights reserved.

Portions Copyright © 1995-1999 LizardTech, Inc. All rights reserved.

Red Hat is a registered trademark of Red Hat, Inc.

Sun is a registered trademark, and Sun ONE, Solaris, iPlanet and Java are trademarks of Sun Microsystems, Inc.

Sybase is a registered trademark of Sybase, Inc.

UNIX is a registered trademark of The Open Group.

Verity is a registered trademark of Autonomy Corporation plc

Index

I

A

about the tutorials, 1-1
account naming conventions, 4-7
accounts, 3-2, 4-2, 4-12
active reports, 5-34
active workflows, 2-6
admin, 3-9, 3-11
administrators, 1-2
aliases, 3-17
all accounts, 4-16
Alternate File, 5-11
audience, 1-2
Author, 5-11

B

basic, 7-10
basic workflows, 8-13
browser configuration, 1-5

C

checked out content, 2-5
checking in, 2-9
checking out, 2-10
Comments, 5-12
config.cfg, 4-9
Configuration Manager, 5-6
Content ID, 5-11
content information fields, 2-8
Content Management, 2-5
content profiles, 6-1
content type, 5-4
contributor, 3-9
conventions, 1-3
criteria subscription, 7-10
criteria workflow, 8-3
custom metadata fields, 5-12

D

database design, 5-17
documents without accounts, 4-16
duration, 1-3

E

exercise 1, 2-14
exercise 2, 3-18
exercise 3, 4-16
exercise 4, 4-21
exercise 5, 5-9
exercise 6, 5-42
Expiration Date, 5-12
expired content, 2-6
External URL, 5-20
external URL, 5-2
external users, 3-14

F

fields
    adding custom user, 3-15
filter content, 7-3

G

global users, 3-14

H

historical reports, 5-35

I

index page, 5-24
information fields
    adding custom user, 3-15