

Folders and WebDAV Administration Guide
10g Release 3 (10.1.3.3.2)

October 2007

Folders and WebDAV Administration Guide, 10g Release 3 (10.1.3.3.2)
Copyright © 2007, Oracle. All rights reserved.

Contributing Author: Ron van de Crommert, Karen Johnson

Contributors: Lyle Sitzman

The Programs (which include both the software and documentation) contain proprietary information; they are provided under a license agreement containing restrictions on use and disclosure and are also protected by copyright, patent, and other intellectual and industrial property laws. Reverse engineering, disassembly, or decompilation of the Programs, except to the extent required to obtain interoperability with other independently created software or as specified by law, is prohibited.

The information contained in this document is subject to change without notice. If you find any problems in the documentation, please report them to us in writing. This document is not warranted to be error-free. Except as may be expressly permitted in your license agreement for these Programs, no part of these Programs may be reproduced or transmitted in any form or by any means, electronic or mechanical, for any purpose.

If the Programs are delivered to the United States Government or anyone licensing or using the Programs on behalf of the United States Government, the following notice is applicable:

U.S. GOVERNMENT RIGHTS Programs, software, databases, and related documentation and technical data delivered to U.S. Government customers are "commercial computer software" or "commercial technical data" pursuant to the applicable Federal Acquisition Regulation and agency-specific supplemental regulations. As such, use, duplication, disclosure, modification, and adaptation of the Programs, including documentation and technical data, shall be subject to the licensing restrictions set forth in the applicable Oracle license agreement, and, to the extent applicable, the additional rights set forth in FAR 52.227-19, Commercial Computer Software--Restricted Rights (June 1987). Oracle USA, Inc., 500 Oracle Parkway, Redwood City, CA 94065.

The Programs are not intended for use in any nuclear, aviation, mass transit, medical, or other inherently dangerous applications. It shall be the licensee's responsibility to take all appropriate fail-safe, backup, redundancy and other measures to ensure the safe use of such applications if the Programs are used for such purposes, and we disclaim liability for any damages caused by such use of the Programs.

Oracle, JD Edwards, PeopleSoft, and Siebel are registered trademarks of Oracle Corporation and/or its affiliates. Other names may be trademarks of their respective owners.

The Programs may provide links to Web sites and access to content, products, and services from third parties. Oracle is not responsible for the availability of, or any content provided on, third-party Web sites. You bear all risks associated with the use of such content. If you choose to purchase any products or services from a third party, the relationship is directly between you and the third party. Oracle is not responsible for: (a) the quality of third-party products or services; or (b) fulfilling any of the terms of the agreement with the third party, including delivery of products or services and warranty obligations related to purchased products or services. Oracle is not responsible for any loss or damage of any sort that you may incur from dealing with any third party.

Table of Contents



Chapter 1: Introduction

Overview	1-1
About this Guide	1-1
Documentation	1-2

Chapter 2: About Folders

Overview	2-1
Folders Overview	2-2
Folders Structure	2-3
Folders Component Security	2-3
Folder Metadata Inheritance	2-4
Trash Bin	2-4
Metadata Propagation	2-5
Folder Content Item Revisions	2-6
Default Metadata Values	2-7
Local Folders	2-8
Folder Archiving	2-10
Folder Searching	2-10

Chapter 3: About WebDAV

Overview	3-1
About WebDAV	3-1
What is WebDAV?	3-2
WebDAV Clients	3-2
WebDAV Architecture	3-3

Security3-4

Chapter 4: Administering Folders

Overview 4-1

Folders Administrator Interface 4-1

 Folder Configuration Link 4-2

 Virtual Folder Administration Configuration Page 4-3

 System Folder Configuration Page 4-4

 System Default Information Field Configuration Page 4-5

 Local Folders Page 4-7

 Information Field Inherit Configuration Page 4-9

Configuring Folders 4-10

 Setting Folder and File Limits 4-10

 Disabling System Folders 4-12

 Enabling System Folders 4-12

 Disabling the Trash Bin 4-13

 Defining System Default Metadata 4-13

 Configuring Metadata Propagation 4-14

 Preventing Folder Static Inheritance for Specific Metadata Fields .. 4-15

 Hiding Metadata Fields Globally Except for Specific Folders 4-16

Working With Local Folders 4-17

 Specifying Local Folders 4-18

 Rebuilding Local Folders 4-18

 Removing Local Folders 4-19

Archiving Folders 4-19

 Exporting an Archive 4-19

 Importing an Archive 4-20

Optimizing System Performance 4-21

Chapter 5: Administering WebDAV

Overview 5-1

Virtual Folders 5-1

Configuring WebDAV 5-2

 Setting WebDAV Title Allocation 5-2

Multiple Concurrent Language Support 5-3

WebDAV Troubleshooting 5-4

 Zero-Byte Files 5-5

 No Connection to WebDAV Virtual Folder 5-5

Double-Byte Characters in File Name 5-6
 Number Sign in Virtual Folder Name or File Name 5-6
 ExtranetLook Component Problem 5-7
 Content Item “Stuck” in Auto-Contribution Workflow Step 5-7
 Deleting Content From Contribution Folders for Site Studio Website . . 5-8
 WebDAV Drag and Drop Does not Work With Windows 2000 5-9
 Profile Rule for All WebDAV Requests 5-10

Appendix A: Third Party Licenses

Overview 6-1
 Apache Software License 6-1
 W3C® Software Notice and License 6-2
 Zlib License 6-4
 General BSD License. 6-5
 General MIT License 6-5
 Unicode License. 6-6
 Miscellaneous Attributions 6-7

Index

INTRODUCTION

OVERVIEW

This section covers the following topics:

- ❖ [About this Guide](#) (page 1-1)
- ❖ [Documentation](#) (page 1-2)

ABOUT THIS GUIDE

This guide explains how to administer Folders and WebDAV.

It is intended for administrators of the Oracle Content DB bundle.



Note: For information about installing and setting up Folders and WebDAV, refer to the *Content Server Folders and WebDAV Installation Guide*.





Conventions

The following conventions are used throughout this document:

- ❖ Forward slashes (/) are used to separate the directory levels in a path name, both for Windows and UNIX. A forward slash always appears after the end of a directory name.
- ❖ The notation *[Instance_Dir]* is used to refer to the location on your system where the Oracle Content Server instance is installed (for example, *C:/Stellent/idm1/*).

Symbols

The following symbols are used throughout this guide:

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

DOCUMENTATION

The following documentation is available for Folders and WebDAV:

- ❖ **Content Server Folders and WebDAV Installation Guide** (*PDF*)
This document provides guidelines and step-by-step procedures for installing and setting up Folders and WebDAV on a content server and client computers.
- ❖ **Content Server Folders and WebDAV Administration Guide** (*HTML and PDF*)
This document provides system management and maintenance information for Folders and WebDAV.
- ❖ **Content Server Folders and WebDAV User Guide** (*HTML and PDF*)
This document provides information to help content consumers and contributors work with Folders and WebDAV effectively.

ABOUT FOLDERS

OVERVIEW

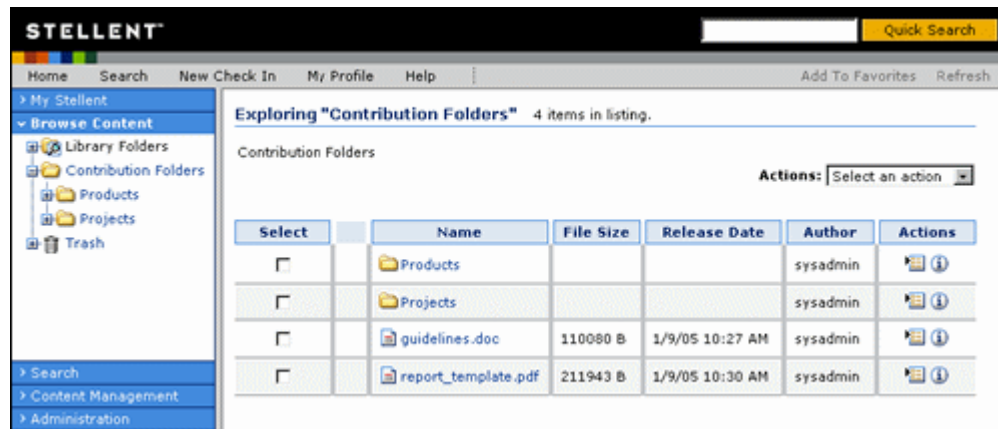
This section covers the following topics:

- ❖ [Folders Overview](#) (page 2-2)
- ❖ [Folders Structure](#) (page 2-3)
- ❖ [Folders Component Security](#) (page 2-3)
- ❖ [Folder Metadata Inheritance](#) (page 2-4)
- ❖ [Trash Bin](#) (page 2-4)
- ❖ [Metadata Propagation](#) (page 2-5)
- ❖ [Folder Content Item Revisions](#) (page 2-6)
- ❖ [Default Metadata Values](#) (page 2-7)
- ❖ [Local Folders](#) (page 2-8)
- ❖ [Folder Archiving](#) (page 2-10)
- ❖ [Folder Searching](#) (page 2-10)

FOLDERS OVERVIEW

Folders is an optional component for use with Content Server that provides a hierarchical folder interface to content in Oracle Content Server in the form of “virtual folders” (also called “hierarchical folders”). Virtual folders enable you to create a multi-level folder structure. Figure 2-1 shows virtual folders as viewed from a content server web page.

Figure 2-1 Virtual folders in Content Server interface (Trays layout with Stellent05 skin)



Virtual folders provide two main benefits:

- ❖ Users can find content by drilling down through a familiar folder-type interface.



Note: Some of the fields in the My View search results are unavailable or not applicable when browsing through virtual folders. For example, if the user enables Vault File Size as a column in their My View, this field will be populated when performing searches, but it will be blank when browsing through virtual folders.

- ❖ Users can apply default metadata to content items by checking them in through a particular folder.
- ❖ The system administrator can control the default metadata applied to content items by appropriately setting up folders.
- ❖ In turn, the preset default metadata is applied to content items when users check them in through a particular folder (set up by the system administrator).

FOLDERS STRUCTURE

The following structure is used for Folders:

- ❖ Each content server instance has a common set of virtual folders. Any change to the folders is applied system-wide.
- ❖ There is one default system-level folder, called *Contribution Folders*.
 - If the Trash Bin function was enabled during installation, a system-level folder called *Trash* is also created.
 - If you are using a custom folders interface, folders for these products may also appear at the system level of the Folders hierarchy.
- ❖ The system administrator can change the name of a system-level folder, but cannot delete it or add a custom system-level folder except through changes to the database. (Deleting a system-level folder disables it, but does not remove it from the system.)
- ❖ Each folder in the hierarchy contains content items that have the same numerical “Folder” value, which is assigned automatically upon creation of the folder. Changing the value of the Folder field for a content item places it in a different folder.
- ❖ The maximum number of folders and content items in each folder can be limited so that browsing through virtual folder does not affect system performance. See [Setting Folder and File Limits](#) (page 4-10) for further details.

FOLDERS COMPONENT SECURITY

The Folders component applies security at two levels:

- ❖ [Content item level](#)
- ❖ [Folder level](#)

Content Item Security

The user logins and security controls in Content Server also apply to content that is managed through virtual folders. For example, if you have Read permission for a content item, you will be able to view the file, but you will not be able to check in a revision to the file.



Note: To allow users with Read permission to access content through a virtual folder, the “Allow get copy for user with read privilege” system property must be enabled. For details, refer to *Content Server Managing System Settings and Processes* guide.

Folder Security

In addition to content item security, Folders also applies security at the folder level:

- ❖ Users can see only the virtual folders that are assigned no security group or a security group for which they have at least Read permission.
- ❖ Each virtual folder has an *owner*, which is a user who has permission to manage the folder. The owner can change a folder’s metadata and delete the folder, even if they do not have Write or Delete permission to the folder’s security group. However, the owner does not have additional permissions to content items within the folder.
- ❖ To change a folder’s default metadata, you must have Delete permission to the folder or you must be the owner of the folder.
- ❖ To delete a folder, you must have Delete permission to the folder or you must be the owner of the folder. You must also have permission to delete all of the content items and subfolders in that folder.



Caution: Be careful when changing the security group of a folder. If you change a folder to a more restrictive security group, authors may no longer have permission to manage their own content items.

FOLDER METADATA INHERITANCE

When you create a new folder, the metadata from the parent folder will populate the fields for the new folder. This allows the folder to initially “inherit” metadata, but allows you to make changes to the new folder.

Subsequent changes to a parent folder’s metadata do not affect the metadata for existing subfolders. If you want to apply a parent folder’s metadata to subfolders and content items, you can use the [Metadata Propagation](#) feature (see page 2-5).

TRASH BIN

The *Trash Bin* function is an optional feature that sends deleted items to a Trash folder, rather than permanently deleting the items. Items in the Trash folder can then be

permanently deleted or restored to their original location in the folder hierarchy. This enables users to recover files and folders that have been mistakenly deleted.

Please note the following considerations with regard to the Trash Bin feature:

- ❖ Deleting a revision from the Repository Manager bypasses the Trash folder and permanently deletes the revision.
- ❖ The Trash Bin function can be enabled during Folders component installation. If it was not enabled during installation and you want to enable it manually, you need to add four configuration settings and metadata fields:

- CollectionTrashDeleter
- CollectionTrashDeleteDate
- CollectionTrashDeleteLocation
- CollectionTrashDeleteOldName

For further details about these configuration settings refer to the *Folders and WebDAV Installation Guide*.

- ❖ If you are using folders to contribute content to a Site Studio website, you may want to disable the Trash Bin feature. Otherwise, any deleted content items (i.e., moved to Trash Bin) will still show up in your tables of contents (dynamic lists) on the website. To get rid of the content items, you need to go into the Trash Bin in WebDAV and explicitly delete the documents from there, too. See [Disabling the Trash Bin](#) (page 4-13) for further instructions.

METADATA PROPAGATION

The *metadata propagation* function enables contributors to copy default metadata values from a folder to its subfolders and content items. Typical uses for this function include:

- ❖ After moving a large number of content items to a new folder structure, you want to apply the top-level folder's default metadata to all subfolders and content items.
- ❖ You revised the default metadata for a folder, and you want to apply it to subfolders and content items within that folder.

Please note the following considerations with regard to metadata propagation:

- ❖ The propagation function applies each folder's metadata to all "uninhibited" subfolders and content items within those folders. This means that each uninhibited subfolder and content item will inherit the metadata of the folder from which propagation was launched.

- ❖ When you inhibit a folder, it is not affected by metadata propagation from a higher-level folder. However, you can still launch metadata propagation *from* an inhibited folder.
- ❖ The system administrator selects which metadata fields are included in propagation. (This is a system-wide setting.) By default, no metadata fields are included until they are selected on the [Information Field Inherit Configuration Page](#) (page 4-9).
- ❖ If a folder metadata field does not have a value defined, subfolders and content items within that folder may not inherit the “blank” value during propagation and any existing metadata values may stay intact for these items. This depends on the value of the `CollectionPropagateEmptyValues` configuration variable, which controls whether empty field values are propagated. For more detailed information about setting this configuration variable, refer to the *Content Server Folders and WebDAV Installation Guide*.
- ❖ When you launch metadata propagation, only folders and content items for which you have Write permission to the security group will be affected.



Note: See [Configuring Metadata Propagation](#) (page 4-14) for more information.

FOLDER CONTENT ITEM REVISIONS

When documents are edited and checked into the content server, the revised document must undergo a process that involves being converted, indexed, and released. Before this process is complete, the system considers the revised document to be the “latest” version. After the process is complete, the system considers the revised document to be the “latest released” version.

Depending on how the version release configuration variable `CollectionReleasedOnly` is set, users with read access to the content item will see either the latest version or nothing at all if the item is not released. Authors, however, will always see the latest version. By default, this variable is enabled and displays the latest version to all users with read access.



Note: For more detailed information about setting the `CollectionReleasedOnly` configuration variable, refer to the *Content Server Folders and WebDAV Installation Guide*.

Latest Version

If the configuration variable `CollectionReleasedOnly` is set to *false*, the visibility of content items is based on the item version rather than the release state. In this case, when a new revision of an existing content item is checked into a folder, the author and all users with read access to the content item are allowed to view the latest version of the revised document.

In the latest version visibility mode, the author and users with read access can view revised items before and after they are converted, indexed, and released. In fact, even if the revised content item fails conversion or indexing, it will still be visible to the author and all users with read access. Additionally, if the release date of the new revision is set to a future date, the revised content item will also be visible to the author and all other users with read access.

Latest Released Version

If the configuration variable `CollectionReleasedOnly` is set to *true*, the visibility of content items is based on the release state rather than the item version. In this case, when a new revision of an existing content item is checked into a folder, the new revision is only visible to the author. The new revision will not become visible to all other users with read access to that content item until it is converted, indexed, and released. This means that until the content item is released, nothing is displayed for non-authoring users. Also, if the release date of the of the new revision is set to a future date, the revised content item will not be visible to other users until that point in time.

DEFAULT METADATA VALUES

When a file is checked into the content server through a virtual folder, default metadata values are entered on the content check-in form automatically. Default metadata values are evaluated in the following order:

1. **Virtual folder default values:**

When you check in a new content item from an Exploring page, any content default metadata values defined for that virtual folder are entered on the content check-in form. These values are defined on the Add/Edit Hierarchy Folder Configuration page, which is described in the *Content Server Folders and WebDAV User Guide*.

2. **User default metadata values:**

If any content metadata defaults are not defined for the virtual folder, the user's default metadata values are applied. These values are defined by each user for new content items on their Default Information Field Configuration page, and for revised content items on their Revision Information Field Configuration page. Both pages are described in the *Content Server Folders and WebDAV User Guide*.



Important: User default metadata values are only applicable when creating new content items using WebDAV. They are not applicable when using the Content Server web interface.

3. **System default metadata values:**

The system default values are applied to any fields that are not defined by the virtual folder or the user's default metadata. These values are defined by the system administrator (see [Defining System Default Metadata](#) on page 4-13).



Important: System default metadata values are only applicable when creating new content items using WebDAV. They are not applicable when using the Content Server web interface.

4. **None:**

A metadata field can be blank as long as it is not a required field. If a required field is left blank, an error will occur and the content item will not be checked in.

LOCAL FOLDERS

The *local folders* function enables you to map a contribution folder structure to a local file system. Changes to the folder, its subfolders, and content items in the content server are reflected in the local directory.

One possible use for this function is to manage a website in the content server but then replicate its structure to a local drive so that hyperlinks are not broken. Because individual files are stored in the content server according to security groups and content types, hyperlinks between web pages would be broken if users attempted to navigate directly from the content items. Also, users would be required to log in and have the appropriate permissions to view each web page.

The following scenario describes how this function could be used to manage a website:

1. A web designer creates a website that contains several web pages with internal hyperlinking in a multi-level directory structure.
2. Through a WebDAV client, the designer copies the entire website structure to a contribution folder called *WebSite*.
3. On the content server's [Local Folders page](#) (see page 4-7), the *WebSite* folder is mapped to a directory on a shared drive, *Z:/Intranet*.
4. The *Intranet* directory is set up as a web server virtual directory.
5. Users can access the website from the *Z:/Intranet* directory without logging in to the content server. Web pages can be updated in the content server, and they will be replicated to the local directory automatically.

Please note the following considerations with regard to local folders:

- ❖ Content server security does not apply to folders or content items in the local directory.
- ❖ Only content items with a status of “Released” will appear in the local directory. Items that fail conversion, are still being indexed, are in a workflow, or have a future release date will not be available in the local directory.
- ❖ Only the latest revision of a content item will be available in the local directory.
- ❖ Modifying directories or files directly in the local file system can cause problems with the local folder mapping. All changes should be made through the content server Folders interface.
- ❖ If you want only users who belong to a specific security group to access specific files, you can point local directories to *weblayout* secured directories.
- ❖ If you move a file from one folder to another (either through the Folders user interface or WebDAV), the copy of that file in the local folder associated with the source folder is not deleted. For example, if you have a folder *WebSite*, files in this folder are automatically copied to its local folder, say, *C:/Website/*. If you now move a file from the folder *WebSite* to another folder, say, *Intranet*, with *Z:/Intranet/* as the local folder, then the file copy in *C:/Website/* is not deleted.



Note: For more information on working with local folders, refer to [Chapter 4 \(Administering Folders\)](#).

FOLDER ARCHIVING

Folders structure and content cannot be archived from one content server to another using the Archiver application. However, you can export and import the folder hierarchy structure directly from the Folders administration interface. You can archive content items separately using Archiver.

Please note the following with regard to folder archiving:

- ❖ Content items must be exported and imported separately using Archiver.
- ❖ When you export the folder hierarchy, the entire structure is exported; you cannot specify a particular folder.
- ❖ The folder hierarchy is exported to a text file that is in HDA format, which can be read by the content server.



Caution: When you import a folder archive file, all current folders and content items are removed from the content server and replaced by the imported folder hierarchy.



Note: For more information on archiving folders, refer to [Chapter 4 \(Administering Folders\)](#).

FOLDER SEARCHING

If the `Folders CollectionSearchRecursiveContent` configuration parameter is set to `true`, then when users click **Search** on the Content Server interface, a Browse button and field will be displayed in the Results Options section of the Search page. The Browse button can be used to find and select a folder, including its subfolders, to be searched.

For further details about this configuration setting refer to the *Folders and WebDAV Installation Guide*.

ABOUT WEBDAV

OVERVIEW

This section covers the following topics:

- ❖ [About WebDAV](#) (page 3-1)
- ❖ [What is WebDAV?](#) (page 3-2)
- ❖ [WebDAV Clients](#) (page 3-2)
- ❖ [WebDAV Architecture](#) (page 3-3)
- ❖ [Security](#) (page 3-4)

ABOUT WEBDAV

WebDAV (Web-Based Distributed Authoring and Versioning) provides a way to remotely author and manage your Oracle content using clients that support the WebDAV protocol. For example, you can use Windows Explorer or Microsoft Office products to check in, check out, and modify content in the Oracle repository rather than using Oracle's web browser interface. WebDAV can be used with Oracle Content Server.



Note: In Content Server, the WebDAV interface is based on the hierarchical Folders interface. See [Chapter 2 \(About Folders\)](#) for more information.



Note: While Folders and WebDAV are separate products, their setup and administration are closely interrelated. The information in this document applies to both products, unless stated otherwise.

WHAT IS WEBDAV?

WebDAV is an extension to the HTTP/1.1 protocol that allows clients to perform remote web content authoring operations. The WebDAV protocol is specified by RFC 2518.0.



Note: See the WebDAV Resources Page at <http://www.webdav.org> for more information.

WebDAV provides support for the following authoring and versioning functions:

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

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



Note: In Content Server, the WebDAV interface is based on the hierarchical folder interface provided by the Folders component.



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

WEBDAV CLIENTS

A WebDAV client is an application that can send requests and receive responses using the WebDAV protocol. Oracle Content Server currently supports the following WebDAV clients:

- ❖ Microsoft Windows Explorer
- ❖ Microsoft Word 2000, 2002 (XP), and 2003
- ❖ Microsoft Excel 2000, 2002 (XP), and 2003
- ❖ Microsoft PowerPoint 2000, 2002 (XP), and 2003

You can use WebDAV virtual folders in Windows Explorer to manage files that were created in a non-WebDAV client, but you cannot use the native application to check content in to and out of the content server repository.



Note: This guide uses the term *WebDAV clients*, which are applications that can send requests and receive responses using the WebDAV protocol, such as Microsoft Windows Explorer or Microsoft Office programs. This is not the same as Oracle WebDAV Client, which is a separate Oracle product that enhances the WebDAV interface to the content server.



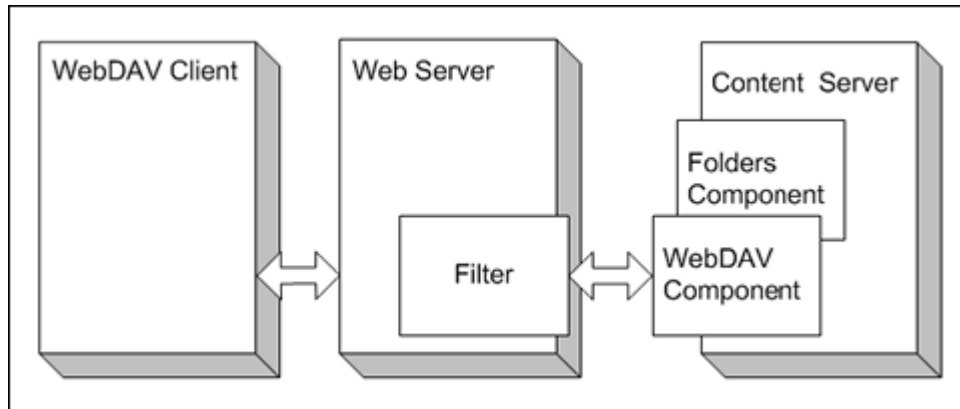
Note: Oracle offers the Desktop Integration Suite, which can enhance your WebDAV client environment by offering integrations into Windows Explorer, Microsoft Outlook, Lotus Notes, and other applications.

WEBDAV ARCHITECTURE

WebDAV support is implemented in the content server through a custom component, which handles WebDAV requests directly. A WebDAV request to the content server follows the following process (as illustrated in Figure 3-1):

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

Figure 3-1 WebDAV process



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

SECURITY

The following security features are included in WebDAV functionality:

- ❖ [Access](#) (page 3-4)
- ❖ [Read-Only Permission](#) (page 3-5)
- ❖ [Login Cookie](#) (page 3-5)
- ❖ [Windows Explorer](#) (page 3-5)
- ❖ [Session Timeout](#) (page 3-5)

Access

The user logins and security controls in the Folders component and Content Server also apply to content that is managed using WebDAV clients. For example, if you have Read permission for a content item, you will be able to view the file, but you will not be able to check in a new revision to the file.

Read-Only Permission

To allow users with only Read permission to access content through a WebDAV client, the “Allow get copy for user with read privilege” feature must be enabled. (You can enable this setting during Folders component installation, in the content server’s System Properties utility, or on the Content Security page of the Admin Server.)

Login Cookie

When a user logs in to the content server through a WebDAV application, the WebDAV component sets a cookie in the client. The cookie remains set as long as a WebDAV request is made within the time specified by the `WebDAVMaxInactiveInterval` parameter in the `[Instance_Dir]/custom/Webdav/webdav_environment.cfg` configuration file. The default is 3600 seconds, or one hour. The cookie will remain set even if the WebDAV client application is closed. If the cookie expires, the user will need to log in to the content server again to perform WebDAV transactions through Microsoft Word, Excel, and PowerPoint.

The cookie includes a cryptographic key that prevents unauthorized users from generating counterfeit cookies. The `WebDAVSecretKey` parameter in the `[Instance_Dir]/custom/Webdav/webdav_environment.cfg` configuration file is used to generate the key.



Tech Tip: To prevent WebDAV login cookies from being used on other content servers, we recommend that you change the `WebDAVSecretKey` setting to a new, unique value for each content server instance that is accessed through WebDAV.

Windows Explorer

If a user logs in to the content server through Windows Explorer, the client retains the user login authentication within the shell. Even if the login cookie expires, Windows Explorer will send the username and password to the content server automatically, so the user will not be prompted to log in. The only way to clear this is for the user to log out of Windows.

Session Timeout

If a WebDAV client does not specify a session timeout value, the default timeout specified by the `WebDAVDefaultTimeout` setting in the `[Instance_Dir]/custom/Webdav/webdav_environment.cfg` configuration file is used. If a file remains locked (checked out) for this amount of time, an “Undo Checkout” is applied to any checked out content.

ADMINISTERING FOLDERS

OVERVIEW

This section covers the following topics:

- ❖ [Folders Administrator Interface](#) (page 4-1)
- ❖ [Configuring Folders](#) (page 4-10)
- ❖ [Working With Local Folders](#) (page 4-17)
- ❖ [Archiving Folders](#) (page 4-19)
- ❖ [Optimizing System Performance](#) (page 4-21)



Note: This guide assumes that your content server is using the Trays layout with the Stellent05 skin, which is the default for Oracle Content Server 10gR3.

FOLDERS ADMINISTRATOR INTERFACE

The Folders component has the following administrative interface features:

- ❖ [Folder Configuration Link](#) (page 4-2)
- ❖ [Virtual Folder Administration Configuration Page](#) (page 4-3)
- ❖ [System Folder Configuration Page](#) (page 4-4)
- ❖ [System Default Information Field Configuration Page](#) (page 4-5)
- ❖ [Local Folders Page](#) (page 4-7)
- ❖ [Information Field Inherit Configuration Page](#) (page 4-9)

Folder Configuration Link

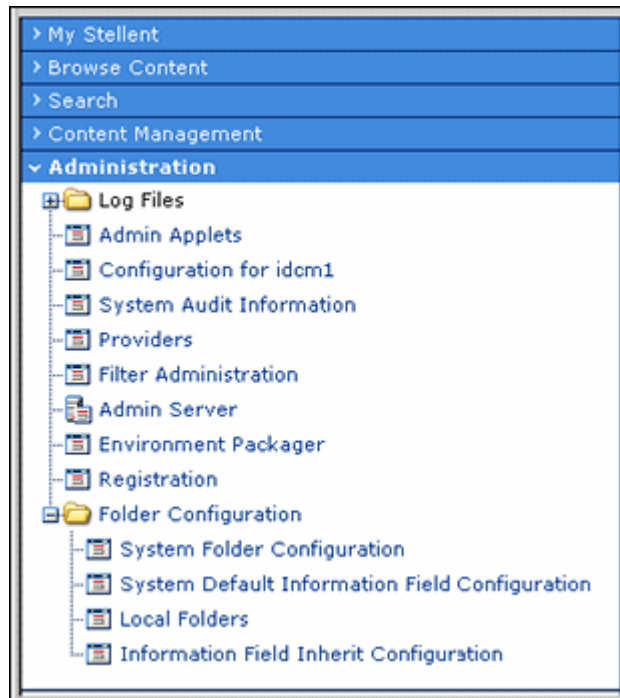
When the Folders component is enabled, a new **Folder Configuration** link appears in the Administration tray.

If you click on this link, the [Virtual Folder Administration Configuration](#) page (see page 4-3) is displayed.

If you expand this link, the following pages are displayed:

- ❖ [System Folder Configuration](#) (see page 4-4)
- ❖ [System Default Information Field Configuration](#) (see page 4-5)
- ❖ [Local Folders](#) (see page 4-7)
- ❖ [Information Field Inherit Configuration](#) (see page 4-9)

Figure 4-1 Folder Configuration link




Virtual Folder Administration Configuration Page

The Virtual Folder Administration Configuration page is used to limit the number of virtual folders and content items in the folders, and provides access to the other Folder system configuration pages. To access this page, click the [Folder Configuration](#) link in the Administration tray.

Figure 4-2 Virtual Folder Administration Configuration page

Feature	Description
Maximum Folders Per Virtual Folder field	Sets the maximum number of virtual folders that any user can define. If a user attempts to define more than this number of virtual folders, the Save command will return an error message.
Maximum Content Per Virtual Folder field	Sets the maximum number of files that any virtual folder can contain.
Update button	Applies the changes to the system.

Feature	Description
Export Archive button	Exports the folder hierarchy as an archive file.
Import Archive button and field	Imports the specified folder archive.  Caution: When you import a folder archive file, all current folders are removed from the content server and replaced by the imported hierarchy.
Browse button	Enables you to select the folder archive file that you want to import.
System Folder Configuration button	Displays the System Folder Configuration page (see page 4-4).
System Default Information Field Configuration button	Displays the System Default Information Field Configuration page (see page 4-5).
Local Folders button	Displays the Local Folders page (see page 4-7).
Information Field Inherit Configuration button	Displays the Information Field Inherit Configuration page (see page 4-9).

See also:

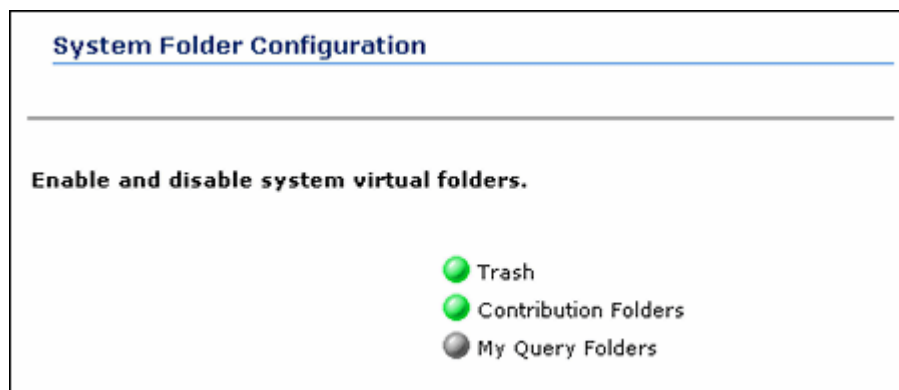
- [Setting Folder and File Limits](#) (page 4-10)
- [Exporting an Archive](#) (page 4-19)
- [Importing an Archive](#) (page 4-20)



System Folder Configuration Page

The System Folder Configuration page is used to enable and disable system-level virtual folders. To access this page, do either of the following:

- ❖ In the Administration tray, expand the [Folder Configuration](#) link (see page 4-2) and click the **System Folder Configuration** link.
- ❖ Click the **System Folder Configuration** button on the [Virtual Folder Administration Configuration](#) page (see page 4-3).

Figure 4-3 System Folder Configuration page



Feature	Description
Enabled/Disabled icon	<p>Clicking an icon displays the associated system folder and enables or disables the folder.</p> <p> (green) = Enabled; users see the folder in the Exploring pages.</p> <p> (gray) = Disabled; users do not see the folder in the Exploring pages.</p>



Important: Query folders are supported only for use with Check Out and Open, and not for other purposes.

See also:

- [Disabling System Folders](#) (page 4-12)
- [Enabling System Folders](#) (page 4-12)
- [Disabling the Trash Bin](#) (page 4-13)

System Default Information Field Configuration Page

The System Default Information Field Configuration page is used to set system default metadata for folders. To access this page, do either of the following:

- ❖ In the Administration tray, expand the [Folder Configuration](#) link (see page 4-2) and click the **System Default Information Field Configuration** link.

- ❖ Click the **System Default Information Field Configuration** button on the [Virtual Folder Administration Configuration](#) page (see page 4-3).

Figure 4-4 System Default Information Field Configuration page

System Default Information Field Configuration

Specify the information field defaults that will be applied for all users.

Type

Security Group

Folder

Comments

Hidden

Read Only

Trash Delete Date


Trash Delete Location

Trash Delete Old Name

Trash Deleter

Release Date

Expiration Date

Feature	Description
Information fields	<p>Define the metadata values that will be applied to content checked in through a virtual folder if values are not already defined for the folder or by the user.</p> <p> Note: These metadata values are applied only on initial check-in; these settings do not affect revisions to existing content.</p> <ul style="list-style-type: none"> • Idoc Script can be used in any of the information fields. • Although the Release Date field is required, the content server will automatically use the current date and time if this field is left blank.
Update button	Applies changes to the system defaults.
Reset button	Resets the fields to the last saved values.

See also:

- [Default Metadata Values](#) (page 2-7)
- [Metadata Propagation](#) (page 2-5)
- [Defining System Default Metadata](#) (page 4-13)

Local Folders Page

The Local Folders page is used to map a contribution folder structure to a local file system. To access this page, do either of the following:

- ❖ In the Administration tray, expand the [Folder Configuration](#) link (see page 4-2) and click the **Local Folders** link.
- ❖ Click the **Local Folders** button on the [Virtual Folder Administration Configuration](#) page (see page 4-3).

Figure 4-5 Local Folders page

The screenshot shows a web interface titled "Local Folders". Below the title is a horizontal line, followed by the instruction "Specify virtual folders to be replicated to directories on host system." Below this is a table with two columns: "Folder" and "Local Directory". The first row of the table contains the text "/Contribution Folders/ » C:\Website" and two buttons: "Rebuild" and "Remove". Below the table is a form with two input fields: "Folder" and "Local Directory". The "Folder" field has a "Browse..." button to its right. Below the input fields is an "Add" button.

Feature	Description
Rebuild button	Deletes the existing local directory structure and recreates the folder structure. Any subdirectories and files will be deleted from and then re-copied to the local directory.
Remove button	Removes the local directory from the file system.
Folder field	The contribution folder to be mapped to a local directory.
Browse button	Displays the Browsing dialog (described in the <i>Content Server Folders and WebDAV User Guide</i>), which is used to select the folder to be mapped to a local directory.
Local Directory field	The directory on a file system where the folder structure will be replicated.
Add button	Replicates the specified folder to the specified directory on the file system.

See also:

- [Local Folders](#) (page 2-8)
- [Specifying Local Folders](#) (page 4-18)
- [Rebuilding Local Folders](#) (page 4-18)
- [Removing Local Folders](#) (page 4-19)

Information Field Inherit Configuration Page

The Information Field Inherit Information page is used to select which metadata values will be propagated from a folder to its subfolders and content items. To access this page, do either of the following:

- ❖ In the Administration tray, expand the [Folder Configuration](#) link (see page 4-2) and click the **Information Field Inherit Configuration** link.
- ❖ Click the **Information Field Inherit Configuration** button on the [Virtual Folder Administration Configuration](#) page (see page 4-3).

Figure 4-6 Information Field Inherit Configuration page

Information Field Inherit Configuration

Select information fields that are to be propagated to content.

- Title
- Author
- Type
- Security Group
- Release Date
- Expiration Date
- Folder
- Comments
- Hidden
- Inhibit Propagation
- Read Only
- Trash Delete Date
- Trash Delete Location
- Trash Delete Old Name
- Trash Deleter

Update Reset

Feature	Description
Information Field check boxes	Selects the metadata fields to be propagated.
Update button	Saves the current settings.
Reset button	Resets the check boxes to their last saved settings.

See also:

- [Folder Metadata Inheritance](#) (page 2-4)
- [Metadata Propagation](#) (page 2-5)
- [Configuring Metadata Propagation](#) (page 4-14)

CONFIGURING FOLDERS

This section covers the following topics:

- ❖ [Setting Folder and File Limits](#) (page 4-10)
- ❖ [Disabling System Folders](#) (page 4-12)
- ❖ [Enabling System Folders](#) (page 4-12)
- ❖ [Disabling the Trash Bin](#) (page 4-13)
- ❖ [Defining System Default Metadata](#) (page 4-13)
- ❖ [Configuring Metadata Propagation](#) (page 4-14)
- ❖ [Preventing Folder Static Inheritance for Specific Metadata Fields](#) (page 4-15)
- ❖ [Hiding Metadata Fields Globally Except for Specific Folders](#) (page 4-16)

Setting Folder and File Limits

If the number of folders and/or content items in a virtual folder is too high, this may affect content server performance. When you browse through folders, each item in a folder is processed by the server, the network, and the client browser. Each item takes a bit of time and resources at each of these steps. The amount of time is dependent on many factors. A fair rule of thumb is that each item will add a few milliseconds to browsing response time and a few kilobytes to the size of the page being displayed in the browser. Please note that the number of items in a folder only affects browsing, not searching.

High numbers of folders and/or content items in a virtual folder also affect the user experience. Users may have a harder time finding things in folders that have a large number of items in them, since they need to browse through a very large list.

It is recommended that you limit the number of folders and content items per virtual folder. The recommended maximum number for both folders and content items per folder is 1,000.



Tech Tip: To improve performance when browsing through folders, you can use set the `CollectionContentSecurity` and `CollectionFolderSecurity` parameters, which reduce security, but speed up browsing. See the *Content Server Folders and WebDAV Installation Guide* for more information on these configuration parameters.



Tech Tip: The more folders you use, the more RAM is required by the folder cache. Therefore, avoid setting up large numbers of unused folders. If you must set up a large number of folders, you should increase the memory for Oracle Content Server. To allocate more memory, you should set the `-Xmx JAVA_OPTIONS` parameter to a high enough value to accommodate the memory requirements and avoid getting an error.

The maximum number of folders and content items in a virtual folder are initially set during the Folders/WebDAV software installation, but it can be modified afterwards:

1. Log in to the content server as an administrator.
2. Open the **Administration** tray.
3. Click the **Folder Configuration** link.

The [Virtual Folder Administration Configuration](#) page (see page 4-3) is displayed.

4. In the **Maximum Folders Per Virtual Folder** field, enter the maximum number of virtual folders allowed.

If a user attempts to define more than this number of virtual folders, an error message is displayed.

5. In the **Maximum Content Per Virtual Folder** field, enter the maximum number of files allowed in each virtual folder.

If a user attempts to check in more than this number of content items, an error message is displayed.

6. Click **Update**.



Note: If you leave the Maximum Folders Per Virtual Folder and the Maximum Content Per Virtual Folder fields blank, all limits are turned off (i.e., there is no maximum). This is not recommended as it affects system performance.

Disabling System Folders

Use the following procedure to disable a system-level virtual folder:

1. Open the file `[Instance_Dir]\custom\Folders\folders_environment.cfg` in a text editor.
2. Make sure the `CollectionReadOnlyMarkedFolders` configuration variable is set to 'false':
`CollectionReadOnlyMarkedFolders=false`
3. If you changed the variable value, save the file and restart the content server.
4. Log into the content server as an administrator.
5. Open the **Administration** tray.
6. Expand the **Folder Configuration** link.
7. Click the **System Folder Configuration** link.

The [System Folder Configuration](#) page (see page 4-4) is displayed.

8. Click the green icon next to the folder you want to disable.

The folder is disabled. Users will not be able to see the disabled folder.

Enabling System Folders

Use the following procedure to enable a system-level hierarchical folder that has been disabled:

1. Open the file `[Instance_Dir]\custom\Folders\folders_environment.cfg` in a text editor.
2. Make sure the `CollectionReadOnlyMarkedFolders` configuration variable is set to 'false':
`CollectionReadOnlyMarkedFolders=false`
3. If you changed the variable value, save the file and restart the content server.
4. Log into the content server as an administrator.
5. Open the **Administration** tray.
6. Expand the **Folder Configuration** link.
7. Click the **System Folder Configuration** link.

The [System Folder Configuration](#) page (see page 4-4) is displayed.

8. Click the gray icon next to the folder you want to enable.

The folder is enabled and the folder Exploring page (described in the *Content Server Folders and WebDAV User Guide*) for the folder is displayed. Users will be able to see the enabled folder.

Disabling the Trash Bin

If you chose to enable the Trash Bin feature during the Folders component installation, a Trash Bin is created, which will contain any content deleted from within Content Server folders. To disable the Trash Bin after the initial Folders setup, complete the following steps:

1. Open the file `[Instance_Dir]\custom\Folders\folders_environment.cfg` in a text editor.
2. Make sure the `CollectionReadOnlyMarkedFolders` configuration variable is set to 'false':

```
CollectionReadOnlyMarkedFolders=false
```
3. If you changed the variable value, save the file and restart the content server.
4. Log into the content server as an administrator.
5. Open the **Administration** tray.
6. Expand the **Folder Configuration** link.
7. Click the **System Folder Configuration** link.
8. Click on the green dot next to Trash. This will disable the Trash Bin.

From now on, any content deleted from Oracle folders will be permanently deleted rather than being moved to the Trash Bin. **This means that content, once deleted, can no longer be restored!**



Note: Disabling the Trash Bin may be particularly useful if you are using Site Studio. See [Deleting Content From Contribution Folders for Site Studio Website](#) (page 5-8) for further details.

Defining System Default Metadata

Use this procedure to define the system default metadata.



Note: Users should still set their own default metadata to ensure that content items do not all have the same metadata. (See the Defining User Metadata Defaults sections in the *Content Server Folders and WebDAV User Guide*).



Note: These defaults will be applied to any content checked in through a virtual folder *only* if a value is not defined for the folder or by the user. See the Defining User Metadata Defaults sections in the *Content Server Folders and WebDAV User Guide* for more information.



Note: These metadata values are applied only on initial check-in; these settings do not affect revisions to existing content.

1. Log in to the content server as an administrator.
2. Open the **Administration** tray.
3. Expand the **Folder Configuration** link.
4. Click the **System Default Information Field Configuration** link.
The [System Default Information Field Configuration](#) page (see page 4-5) is displayed.
5. Specify the default values to be applied to content upon check-in.



Note: Idoc Script can be used in any information field.

6. Click **Update**.

Configuring Metadata Propagation

Use the following procedure to specify which metadata values will propagate to subfolders and content items when a contributor launches the [Metadata Propagation](#) (page 2-5) function:

1. Log in to the content server as an administrator.
2. Open the **Administration** tray.
3. Expand the **Folder Configuration** link.
4. Click the **Information Field Inherit Configuration** link.
The [Information Field Inherit Configuration](#) page (see page 4-9) is displayed.
5. Select check boxes for the metadata fields to be propagated.
6. Click **Update**.

When a contributor clicks the Propagate button on a Hierarchical Folder Information page (described in the *Content Server Folders and WebDAV User Guide*), only the selected metadata values will be propagated.



Tech Tip: You can propagate the “inhibit” setting itself by selecting the check box for the Inhibit Metadata Update field on the Information Field Inherit Configuration page.

However, the “inhibit” setting will only propagate from *false* to *true* or *blank*, and not from *true* or *blank* to *false*. This is because any folders and content items that are already set to *true* or *blank* will not be included in the propagation process.



Tech Tip: You can use the `CollectionPropagateEmptyValues` configuration variable to inhibit propagation of empty field values. For more detailed information about setting this configuration variable, refer to the *Content Server Folders and WebDAV Installation Guide*.



Note: See [Metadata Propagation](#) (page 2-5) and Propagating Metadata (described in the *Content Server Folders and WebDAV User Guide*) for more information on metadata propagation.

Preventing Folder Static Inheritance for Specific Metadata Fields

Oracle Folders uses static inheritance—that is, when you create a new folder or check in new content into a folder, the metadata from the parent folder will automatically populate the fields for the new folder or the new content item. This allows the folder to initially “inherit” metadata, but allows you to make changes to the new folder. Subsequent changes to a parent folder’s metadata do not affect the metadata for existing subfolders or content checked into a folder.

There are cases where you do not want items checked into a folder to inherit the parent folder’s metadata values. For example, you might want to create a folder with the metadata field of `ReadOnly` set to a value of “true”. Setting this value to “true” on the folder prevents renaming, moving, or deleting the folder; however, content can still be checked into the folder. If the content checked into the folder inherits the folder’s metadata value of “true” for the `ReadOnly` field, that means that the content cannot be deleted, even by its author. You may want to have a folder set to `ReadOnly`, but you may want any content checked into the folder to not inherit the value of “true” for `ReadOnly` so that deletions are allowed.

You can change the value of the `ReadOnly` field to “false” for content checked into the folder on the checkin page through the browser interface, but if you check in content through WebDAV, there is no way to change the value of this field at check-in time.

In order to prevent the ReadOnly field from inheriting its value from the parent folder, complete the following steps (this can be used for any metadata field; the ReadOnly field is only used as an example):

1. Locate the `[Install_Dir]/custom/Folders/resources` directory.
2. Copy the existing `folders_forcemeta_resource.hda` file to another name as backup.
3. Open the `folders_forcemeta_resource.hda` file in a text editor.
4. Add another entry to the METADATA_OVERRIDE result set for the metadata field `xReadOnly`. The result set will look like this:

```
@ResultSet METADATA_OVERRIDE
2
name
value
CollectionInhibitUpdateMeta
xReadOnly
@end
```

5. Save the `folders_forcemeta_resource.hda` file.
6. Restart the content server.

Hiding Metadata Fields Globally Except for Specific Folders

Use the following procedure to hide one or more metadata fields globally for all folders and for new check-ins, but allow those metadata fields to be visible for checking in content using specific WebDAV contribution folders.

1. Log in to the content server as an administrator.
2. Open the **Administration** tray.
3. Select the **Admin Applets** link.
4. Select the **Configuration Manager** link.
5. Click the **Rules** tab.
6. Click **Add** to add a rule, then enter information for the rule name and description.
7. In the General tab, select the **is Global rule with Priority** and **Use rule activation condition** check boxes.
 - a. Select **Edit** next to the **User rule activation condition** check box.
 - b. Click **Add** to add a condition.

- c. Make sure the condition is highlighted and select the **Clause** tab.
 - d. In the **Field** menu, select **Folder**.
 - e. In the **Operator** menu, select **Not Equals**.
 - f. In the **Value** menu, enter the xcollectionID of the folder where you want the metadata field to appear. The xcollectionID can be found in the database, in the Collections table under dCollectionID.
 - g. Click **Add** to add the clause to the Clause section.
 - h. Click **OK**.
8. Select the **Fields** tab from the main **Edit Rule** window.
 9. Click **Add**, and select the field you want to hide.
 10. Click **OK**.

The **Add Rule Field** window is displayed.

11. In the **Type** menu of the **Add Rule Field** window, select **Hidden**.
12. Click **OK**.
13. In the main **Edit Rule** window, click **OK**.
14. Test the configuration by adding content to a non-specified folder, The field should be hidden. Try adding content to the folder specified in the rule that you created; the desired field should be visible.



Note: If more than one folder is needed to display the desired fields, more conditions are needed within the clause of the same rule.

WORKING WITH LOCAL FOLDERS

This section covers the following topics:

- ❖ [Specifying Local Folders](#) (page 4-18)
- ❖ [Rebuilding Local Folders](#) (page 4-18)
- ❖ [Removing Local Folders](#) (page 4-19)



Note: Refer to [Local Folders](#) (page 2-8) for more details on local folders.

Specifying Local Folders

Use the following procedure to map a contribution folder structure to a local file system:

1. Log in to the content server as an administrator.
2. Open the **Administration** tray.
3. Expand the **Folder Configuration** link.
4. Click the **Local Folders** link.

The [Local Folders](#) page (see page 4-7) is displayed.

5. Click **Browse**.

The Browsing dialog (described in detail in the *Content Server Folders and WebDAV User Guide*) is displayed.

6. Click the folder to be mapped to the file system. (You may need to navigate to a higher-level folder to display its subfolders.) The target folder is the open folder.
7. Click **OK**.

The target folder is entered in the Folder field.

8. Enter a directory name in the Local Directory field.

For example, *c:/my_website*.

9. Click **Add**.

If necessary, the directory is created on the file system, and the specified folder structure is replicated to the specified directory.

Rebuilding Local Folders

Use the following procedure to rebuild the directory structure for a folder that is mapped to a local file system:

1. Log in to the content server as an administrator.
2. Open the **Administration** tray.
3. Expand the **Folder Configuration** link.
4. Click the **Local Folders** link.

The [Local Folders](#) page (see page 4-7) is displayed.

5. Click **Rebuild** for the folder/directory mapping you want to rebuild.

The directory (and all subdirectories and files) is deleted from the local file system, and the folder structure is re-copied to the directory.

Removing Local Folders

Use the following procedure to delete a local folder mapping:

1. Log in to the content server as an administrator.
2. Open the **Administration** tray.
3. Expand the **Folder Configuration** link.
4. Click the **Local Folders** link.

The [Local Folders](#) page (see page 4-7) is displayed.

5. Click **Remove** for the folder/directory mapping you want to delete.

The directory (and all subdirectories and files) is deleted from the local file system, and the mapping is removed from the Local Folders page.



Note: A mapped virtual folder cannot be deleted until the local folder mapping is removed.

ARCHIVING FOLDERS

This section covers the following topics:

- ❖ [Exporting an Archive](#) (page 4-19)
- ❖ [Importing an Archive](#) (page 4-20)



Note: Refer to [Folder Archiving](#) (page 2-10) for more details on archiving folders.

Exporting an Archive



Note: Depending on the size of the folder hierarchy that is being exported as an archive file, the default heap size value for the JVM may not be adequate. If memory errors are issued during the export procedure, the heap size may need to be increased. For more detailed information about JVM heap size issues, refer to the Archiver chapter in the *Content Server Troubleshooting Guide*.

Use the following procedure to export the folder hierarchy as an archive file:

1. Log in to the content server as an administrator.
2. Open the **Administration** tray.
3. Click the **Folder Configuration** link.
The [Virtual Folder Administration Configuration](#) page (see page 4-3) is displayed.
4. Click **Export Archive**.
A File Download window is displayed.
5. Click **Save**.
A Save As window is displayed.
6. Navigate to the directory where you want to save the folder archive file.
7. Specify a new file name so that you can easily identify the archive file (for example, *041127_CollectionArchive*).
8. Click **Save**.
The folder hierarchy is exported to the specified file.

Importing an Archive

Use the following procedure to import an archived folder structure:



Caution: This procedure removes all current folders and replaces them with the imported folder hierarchy. Typically, you should perform this procedure only on a content server that has no content items in the repository.

1. Log in to the content server as an administrator.
2. Open the **Administration** tray.
3. Click the **Folder Configuration** link.
The [Virtual Folder Administration Configuration](#) page (see page 4-3) is displayed.
4. Click **Browse** and navigate to the archive file you want to import.
5. Click **Open**.
The path and file name appear in the field.

6. Click **Import Archive**.

A confirmation prompt is displayed.

7. Click **OK**.

The archived folder is imported and recreated.

OPTIMIZING SYSTEM PERFORMANCE

Folders performance depends on many different factors. This section provides some guidelines and configuration parameters that can improve content server performance with Folders and WebDAV enabled:

- ❖ **Limit the number of virtual folders, especially unused ones.**

The more folders you use, the more RAM is required by the folder cache. Therefore, avoid setting up large numbers of folders, especially unused ones. If you must set up a large number of folders, you should increase the memory available to Content Server. To allocate more memory, you should set the `-Xmx JAVA_OPTIONS` parameter to a high enough value to accommodate the memory requirements and avoid getting errors.

- ❖ **Limit the number of folders and content items in virtual folders.**

If the number of folders and/or content items in a virtual folder is too high, this may affect content server performance. When you browse through folders, each item in a folder is processed by the server, the network, and the client browser. Each item takes a bit of time and resources at each of these steps. The amount of time is dependent on many factors. A fair rule of thumb is that each item will add a few milliseconds to browsing response time and a few kilobytes to the size of the page being displayed in the browser. Please note that the number of items in a folder only affects browsing, not searching.

High numbers of folders and/or content items in a virtual folder also affect the user experience. Users may have a harder time finding things in folders that have a large number of items in them, since they need to browse through a very large list.

It is therefore recommended that you limit the number of folders and content items per virtual folder. The recommended maximum number for both folders and content items per folder is 1,000. You are prompted to specify these limits during the Folders/WebDAV software installation, but you can also modify them afterwards (see [Setting Folder and File Limits](#) on page 4-10 for details).

- ❖ **Use the Classic view rather than the Headline view for search results.**

Using the Classic view instead of the Headline view can speed up browsing when there are large numbers of items in folders. The Classic view has less functionality so the pages are smaller and simpler. Most of the functionality that is missing in the Classic view is available through the information pages, so additional clicks are required but browsing is faster.
- ❖ **Perform regular database maintenance.**

When there are large numbers of content items and folders in a system, Folders performance is strongly affected by the RDBMS performance. It is helpful to perform periodic (say, monthly) maintenance on the database to make sure there is enough RAM, the database indexes are optimized, and the database is not too fragmented.
- ❖ **Relax security to allow users without the appropriate access privileges to see (but not access!) secure content or folders.**

The configuration variables `CollectionContentSecurity` and `CollectionFolderSecurity` control whether users can see secure content or folders on Exploring pages if they have no access privileges to the secure content or folders. If these variables are set to 'false' (which is not the default), then users with no access privileges to secure content items or folders will see them on Exploring pages. However, if they try to view the content, an "access-denied" error is displayed. This setting speeds up browsing performance as it simplifies the queries that need to be executed (less filtering), but it does allow users to see some information about secure content that they do not have access to.
- ❖ **Limit the number of items and folders that are displayed on Exploring pages.**

You can set the configuration variable `CollectionDisplayResultSetSize` to control the maximum number of items that are displayed on Exploring pages (applicable only when Folders is installed on Content Server 7.x and 10gR3). If the number of items in the result set exceeds the specified number, the results are truncated and spread out over multiple pages. Navigation links are then provided to move between pages. This setting can be useful to prevent extremely large pages from being generated if there are many items to display.
- ❖ **Remove certain options from the Actions popup menu for items on Exploring pages.**

There are a number of configuration variables that remove certain menu options from the Actions popup menu next to the Info icons on Exploring pages. They are `CollectionInfoEnabled:actionPopup` (Folder Information and Content Information options), `CollectionLinkEnabled:actionPopup` (Create Shortcut option),

CollectionMoveEnabled:actionPopup (Move option), and
CollectionDeleteEnabled:actionPopup (Delete option). These settings can greatly reduce the size of the display pages that are constructed, which subsequently load faster (applicable only when Folders is installed on Content Server 7.x and 10gR3).



Note: Refer to the *Content Server Folders and WebDAV Installation Guide* for details on setup and behavior of the configuration parameters mentioned above.

ADMINISTERING WEBDAV

OVERVIEW

This section covers the following topics:

- ❖ [Virtual Folders](#) (page 5-1)
- ❖ [Configuring WebDAV](#) (page 5-2)
- ❖ [Multiple Concurrent Language Support](#) (page 5-3)
- ❖ [WebDAV Troubleshooting](#) (page 5-4)

VIRTUAL FOLDERS



Note: In Oracle Content Server, the WebDAV interface is based on the hierarchical Folders interface. See [Chapter 2 \(About Folders\)](#) for more information.

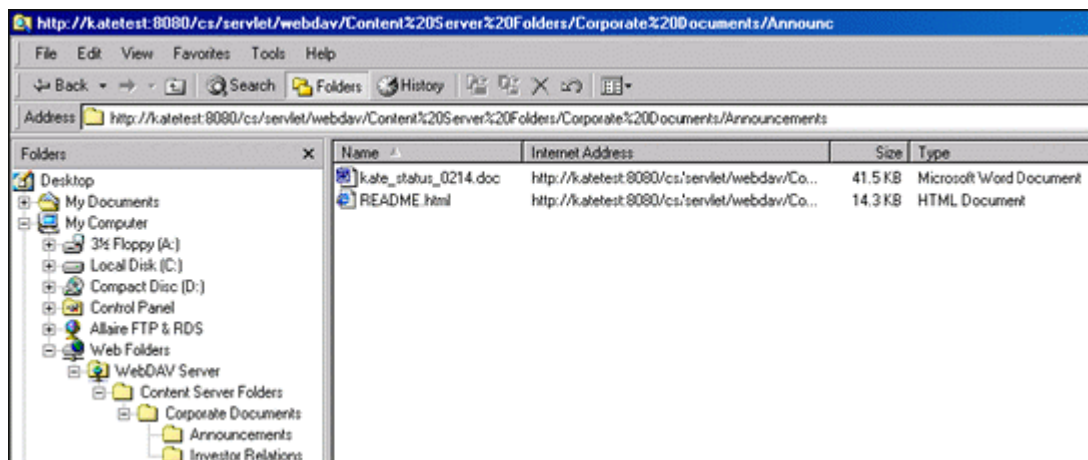
The WebDAV interface to a content server repository is set up as “virtual folders.” Each folder contains the content items that have the same numerical “Folder” value, which is assigned automatically upon creation of the folder.

You can work with content items and virtual folders in much the same way you would work with files and folders in a file system. However, typical tasks you perform on files in a file system may have a different effect when you perform them on files in a WebDAV virtual folder. For example, opening a file from a WebDAV virtual folder also checks the content item out of the content server.

The user logins and security controls in Oracle Content Server and the Folders component also apply to content that is managed using WebDAV clients. For example, if you have Read permission for a content item, you will be able to view the file, but you will not be able to check in a revision to the file.

Figure 5-1 shows how a typical set of WebDAV virtual folders would look in Windows Explorer:

Figure 5-1 WebDAV virtual folders in Windows Explorer



CONFIGURING WEBDAV

After you have installed WebDAV functionality on your content server, most of the WebDAV system administration tasks are performed from Folders component web pages. See [Chapter 4 \(Administering Folders\)](#) for further details.

Setting WebDAV Title Allocation

When users check new content into the content server through WebDAV, they cannot specify a title for the content item. The title is assigned automatically. Use the following procedure to specify how the title allocation is handled:

1. Open the file `[Instance_Dir]\custom\WebDAV\webdav_environment.cfg` in a text editor.

2. Set the `WebDAVDoNotSetTitleToOriginalName` parameter in accordance with the desired title allocation behavior (see below):

```
WebDAVDoNotSetTitleToOriginalName=false|true
```

(The default is ‘false’.)

3. If you changed the variable value, save the file and restart the content server.

The title of content items checked into the content server through WebDAV is now assigned as follows:

- ❖ If the `WebDAVDoNotSetTitleToOriginalName` parameter is set to ‘false’, the file name *without* the file extension is used as the title (for example, “monthly_report”). This is the naming convention regardless of whether a default title metadata value has been defined for the folder.
- ❖ If the `WebDAVDoNotSetTitleToOriginalName` parameter is set to ‘true’ and no default title metadata value has been defined for the folder, the file name *with* the file extension is used as the title (for example, “monthly_report.doc”).
- ❖ If the `WebDAVDoNotSetTitleToOriginalName` parameter is set to ‘true’ and a default title metadata value has been defined for the folder, the defined name is used as the title (for example, “Monthly Report”).



Note: For further information on defining default metadata values for folders refer to the *Content Server Folders and WebDAV User Guide*.

MULTIPLE CONCURRENT LANGUAGE SUPPORT

This section describes the requirements for those who wish to have multiple concurrent language support (for example, both English and Japanese).

To support multiple concurrent languages, certain WebDAV properties (metadata fields) must not contain non-ASCII characters. If non-ASCII characters are used, WebDAV clients may not be able to list folders containing these characters. For example, an English desktop would have trouble displaying Japanese characters.

The specific fields that must not use non-ASCII character sets vary by WebDAV client. This is a listing of the different clients and the metadata fields that must not contain non-ASCII characters:

Microsoft Web Folders

The following fields must not contain non-ASCII characters:

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

Stellent Desktop Integration Suite

The following fields must not contain non-ASCII characters:

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

WEBDAV TROUBLESHOOTING

This section describes problems that may occur when using WebDAV and offers possible solutions.

- ❖ [Zero-Byte Files](#) (page 5-5)
- ❖ [No Connection to WebDAV Virtual Folder](#) (page 5-5)
- ❖ [Double-Byte Characters in File Name](#) (page 5-6)
- ❖ [Number Sign in Virtual Folder Name or File Name](#) (page 5-6)
- ❖ [ExtranetLook Component Problem](#) (page 5-7)
- ❖ [Content Item “Stuck” in Auto-Contribution Workflow Step](#) (page 5-7)
- ❖ [Deleting Content From Contribution Folders for Site Studio Website](#) (page 5-8)

- ❖ [WebDAV Drag and Drop Does not Work With Windows 2000](#) (page 5-9)
- ❖ [Profile Rule for All WebDAV Requests](#) (page 5-10)



Tech Tip: See the content server logs for error messages and detailed information about the operation of the WebDAV component.

Zero-Byte Files

Problem

When using an Office 2000 application to open a document that resides on a WebDAV server, the application displays the content as empty (0 bytes).

Cause

This problem may be caused by a combination of the temporary Internet files settings in Microsoft Internet Explorer. The WebDAV file is still present in the content server, but does not open properly on certain client machines with particular settings.

Solution

1. In Internet Explorer, select **Tools—Internet Options**.
2. On the General tab, click **Settings**.
3. Under “Check for newer versions of stored pages”, select **Every visit to the page**.
4. Under “Temporary Internet files folder”, consider increasing the amount of disk space. (The lower the amount, the sooner the empty file problem seems to occur.)
5. Click **OK** twice to save the settings and close the Internet Options screen.

No Connection to WebDAV Virtual Folder

Problem

A client machine will not connect to WebDAV virtual folders.

Cause

Internet Explorer is configured to use a proxy server. (In Internet Explorer, the “Use a Proxy Server for your LAN” check box under **Tools—Internet Options—Connections—LAN Settings** is selected.)

Solution

Do one of the following:

- ❖ Configure the client machine to not use the proxy server instance for your HTTP server/WebDAV server. To do this in Internet Explorer, select **Tools—Internet Options—Connections—LAN Settings—Advanced—Exceptions**, and specify the IP address/host name of the WebDAV server.
- ❖ Modify the proxy server configuration to allow pass-through for WebDAV methods (WebDAV-specific HTTP/1.1 extensions) along with standard GET, POST, and other HTTP/1.1 methods. Refer to your proxy server documentation for more information.

Double-Byte Characters in File Name

Problem

A file with double-byte characters in the file name cannot be checked in.

Cause

If the content server is running on a Western European operating system, the Microsoft WebDAV client may not be able to handle files with double-byte characters in the file name.

Solution

Either eliminate all double-byte characters from the file name, or check in the file through the content server's web browser interface.

Number Sign in Virtual Folder Name or File Name

Problem

Using the number sign (#) in a virtual folder name generates errors and/or truncates the folder name prior to the number sign. Using the number sign (#) in file names generates errors.

Cause

The the number sign (#) is an illegal WebDAV character.

Solution

Eliminate the number sign (#) from the virtual folder name. Either eliminate the number sign from the file name, or check in the file through the content server's web browser interface.

ExtranetLook Component Problem

Problem

The ExtranetLook component no longer works after installation of the Folder component.

Cause

The WebDAV component uses *CookieLoginPlugin.dll* for cookie-based login. The cookies eliminate additional login prompts when MS-Word opens a document using webdav. Typically, the component keeps the dll from doing forms-based logins on web page because most users do not want this. However, users that do want forms-based logins can get them by following the instructions below.

Solution

An additional configuration change must be made to allow forms-based login with the webdav component. Specifically, if you want to use the WebDAV component along with the ExtranetLook component, you have to change *[Instance_Dir]/custom/Webdav/webdav_environment.cfg* by setting *WebDAVDisableOtherFilterCookies=false* instead of true (the default).

Content Item “Stuck” in Auto-Contribution Workflow Step

Problem

I dragged and dropped a content item into a virtual folder, and the content item automatically entered a workflow (as expected). However, the content item seems “stuck” in the auto-contribution step of the workflow. The only way for me to approve the content item is to check it out and check it back in with the “Revision Finished Editing” option selected, so that the content item will move to the first step of the workflow.

Cause

A change was made to the default workflow behavior when content items are contributed through the WebDAV interface. In Folders revision 91 and higher, a content item enters a workflow in the contribution step when contributed to a virtual folder rather than the first step in the workflow, which used to be the default. This was done to cater to Site Studio's preview modes, so that a content item did not advance into the workflow proper and it could be approved using the Site Studio interface. However, if you are not using Site Studio, this may not be the behavior you are looking for.

Solution

Two Content Server configuration entries are available to address this issue and also to allow for some more functionality:

- ❖ **AutoContributorAdvancesOnUnlock:**
Enabling this configuration entry makes the content advance immediately to the first workflow step as it did in versions of the Folders component prior to revision 91.
- ❖ **AutoContributorAllowsReview:**
This configuration entry enables users to approve a content item in a contribution step of a workflow without having to perform a check-out/check-in sequence.

Deleting Content From Contribution Folders for Site Studio Website

Problem

When I delete documents from folders that I am using to contribute to my Site Studio website, those documents still show up in my tables of contents (dynamic lists) on the website.

Cause

If you chose to enable the Trash Bin feature during the Folders component installation, a Trash Bin is created, which will contain any content deleted from within Content Server folders. This can have an undesirable side-effect when using Site Studio in that documents that are deleted from WebDAV folders will still show up in Site Studio dynamic lists (such as tables of content) and queries, as they are still present in the Trash Bin. You need to explicitly delete the documents from the Trash Bin to make them disappear from all dynamic lists and queries of your Site Studio website.

Solution

To avoid having to delete the documents twice, you can [disable the Trash Bin](#) (see page 4-13). **Please note that after you disable the Trash Bin, the documents, once deleted, cannot be restored!**

WebDAV Drag and Drop Does not Work With Windows 2000

Problem

Attempting to drag and drop using any WebDAV client produces no file, or a file containing 0 bytes. Although the action does not successfully complete, no error message is displayed. A copy and paste of the file using the WebDAV client does work.

Cause

The problem is a known issue on some versions of Windows 2000 with Office 2000 Service Release 1 or later which have been upgraded.

Solution

The following solutions can be used to work around or resolve the drag and drop issue:

- ❖ You can use copy and paste to add content in situations where the drag and drop does not work.
- ❖ You can also upgrade your Windows dll files as outlined in the following Microsoft knowledgebase article:
<http://support.microsoft.com/default.aspx?scid=kb;en-us;288440>

Profile Rule for All WebDAV Requests

Problem

How do I create a profile rule that affects all WebDAV requests?

Solution

Check for the variable `IsWebdavRequest` in your profile rule. For example, you can use the following script for the `dOutDate` field to make sure it is set to 30 days in the future for all WebDAV checkins:

```
<$if IsWebdavRequest$>  
<$dprDerivedValue=dateCurrent(30)$>  
<$endif$>
```



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 6-1)
- ❖ [W3C® Software Notice and License](#) (page 6-2)
- ❖ [Zlib License](#) (page 6-4)
- ❖ [General BSD License](#) (page 6-5)
- ❖ [General MIT License](#) (page 6-5)
- ❖ [Unicode License](#) (page 6-6)
- ❖ [Miscellaneous Attributions](#) (page 6-7)

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.

Third Party Licenses

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



A

- access control of WebDAV, 3-4
- administration
 - Folders, 4-1
 - WebDAV, 5-1
- allocation of content title (WebDAV), 5-2
- architecture of WebDAV, 3-3
- archiving folders, 2-10, 4-19
 - exporting folder hierarchy, 4-19
 - importing folder hierarchy, 4-20
- ASCII characters in WebDAV properties, 5-3

B

- browsing and system performance, 4-21
- browsing performance, 4-10

C

- clients for WebDAV, 3-2
- CollectionContentSecurity, 4-11
- CollectionDisplayResultSetSize, 4-11
- CollectionFolderSecurity, 4-11
- CollectionReleasedOnly, 2-6
- components
 - ExtranetLook, 5-7
- configuration
 - disabling system folders, 4-12
 - enabling system folders, 4-12
 - Folder Configuration link, 4-2
 - Folders, 4-10
 - Information Field Inherit Configuration, 4-9
 - Local Folders, 4-7
 - local folders, 4-17
 - maximum number of folders and files, 4-10
 - metadata propagation, 4-14

- System Default Information Field Configuration, 4-5
- system default metadata, 4-13
- System Folder Configuration page, 4-4
- Virtual Folder Administration Configuration page, 4-3
- WebDAV, 5-2
- configuration parameters
 - CollectionContentSecurity, 4-11
 - CollectionDisplayResultSetSize, 4-11
 - CollectionFolderSecurity, 4-11
 - CollectionReleasedOnly, 2-6
 - WebDAVDoNotSetTitleToOriginalName, 5-2
- connection issues to WebDAV virtual folder, 5-5
- content items
 - revisions, 2-6
 - security, 2-3
 - WebDAV and workflows, 5-7
- cookies
 - login -- (WebDAV), 3-5

D

- default metadata, 2-7, 2-7
 - defining system --, 4-13
 - evaluation order, 2-7, 2-7
- disabling
 - system folders, 4-12
- disabling the Trash Bin, 4-13
- documentation for Folders and WebDAV, 1-2
- double-byte characters in file names, 5-6

E

- enabling
 - system folders, 4-12
- exporting archives, 4-19
- ExtranetLook component, 5-7

F

file system

mapping local folders to --, 4-18

files

double-byte characters in file name, 5-6
maximum number, 4-10
number sign in file name, 5-6
zero bytes, 5-5

Folder Configuration link, 4-2

Folders

administration, 4-1
configuration, 4-10
content item revisions, 2-6
documentation, 1-2
improving performance, 4-21
overview, 2-2
security, 2-3
structure, 2-3
Trash Bin, 2-4
user interface, 4-1

folders

see also 'local folders'
see also 'virtual folders'
archiving, 2-10, 4-19
benefits, 2-2
contribution -- for Site Studio website, 5-8
disabling system --, 4-12
enabling system --, 4-12
exporting --, 4-19
importing --, 4-20
maximum number, 4-10
metadata inheritance, 2-4
security, 2-4

H

hierarchical folders, see 'virtual folders'

HTTP methods used by WebDAV, 3-4

I

importing archives, 4-20

improving system performance, 4-21

Information Field Inherit Configuration page, 4-9

information fields, see also 'metadata'

inheritance of metadata, 2-4, 4-15

interface, see 'user interface'

L

language support, 5-3

latest released versions of content items, 2-7

latest versions of content items, 2-7

links

Folder Configuration, 4-2

local folders, 2-8

configuration, 4-7, 4-17

mapping --, 4-18

rebuilding --, 4-18

removing --, 4-19

Local Folders page, 4-7

login cookie, 3-5

M

mapping local folders, 4-18

maximum number of folders and files, 4-10

metadata

default values, 2-7, 2-7

defining system default --, 4-13

evaluation order, 2-7, 2-7

inheritance, 2-4, 4-15

propagation, 2-5, 4-14

N

non-ASCII characters in WebDAV properties, 5-3

number sign, in virtual folder name or file name, 5-6

O

optimizing system performance, 4-21

P

pages

Information Field Inherit Configuration, 4-9

Local Folders, 4-7

System Default Information Field Configuration, 4-5

System Folder Configuration, 4-4

Virtual Folder Administration Configuration, 4-3

performance of Folders, improving --, 4-21

process of WebDAV requests, 3-3

propagation of metadata, 2-5, 4-14

protocol used by WebDAV, 3-2

Q

query folders, 4-5

R

- read-only permission, 3-5
- rebuilding local folders, 4-18
- removing local folders, 4-19
- revisions of content items
 - latest released versions, 2-7
 - latest versions, 2-7

S

- security
 - content items, 2-3
 - folders, 2-4
 - relaxing -- to improve performance, 4-11
- security of WebDAV, 3-4
 - access control, 3-4
 - login cookie, 3-5
 - read-only permission, 3-5
 - session timeout, 3-5
 - Windows Explorer, 3-5
- session timeout, 3-5
- Site Studio
 - and WebDAV, 2-5, 4-13, 5-8
- static inheritance, preventing --, 4-15
- structure of Folders, 2-3
- System Default Information Field Configuration page, 4-5
- system default metadata, 4-13
- System Folder Configuration page, 4-4
- system folders
 - disabling, 4-12
 - enabling, 4-12
- system performance, 4-21

T

- timeouts
 - WebDAV sessions, 3-5
- title allocation (WebDAV), 5-2
- Trash Bin, 2-4
 - disabling --, 4-13
- troubleshooting
 - connection issues to WebDAV virtual folder, 5-5
 - content items "stuck" in workflow, 5-7
 - deleting content from Site Studio contribution folders, 5-8
 - double-byte characters in file name, 5-6
 - ExtranetLook component, 5-7
 - number sign in virtual folder name or file name, 5-6
 - WebDAV, 5-4
 - WebDAV drag and drop does not work with Windows 2000, 5-9

- zero-byte files, 5-5

U

- user interface (Folders), 4-1
 - Folder Configuration link, 4-2
 - Information Field Inherit Configuration page, 4-9
 - Local Folders page, 4-7
 - System Default Information Field Configuration page, 4-5
 - System Folder Configuration page, 4-4
 - Virtual Folder Administration Configuration page, 4-3
- user interface (WebDAV)
 - virtual folders in Windows Explorer, 5-1

V

- variables, see 'configuration parameters'
- Virtual Folder Administration Configuration page, 4-3
- virtual folders, 2-2, 5-1
 - benefits, 2-2
 - connection issues, 5-5

W

- WebDAV
 - administration, 5-1
 - architecture, 3-3
 - clients, 3-2
 - configuration, 5-2
 - documentation, 1-2
 - functions, 3-2
 - HTTP methods used, 3-4
 - multiple concurrent language support, 5-3
 - overview, 3-1
 - process, 3-3
 - protocol, 3-2, 3-4
 - security, 3-4
 - and Site Studio, 5-8
 - technology, 3-2, 3-3
 - title allocation, 5-2
 - troubleshooting, 5-4
 - troubleshooting drag and drop functionality with Windows 2000, 5-9
 - workflows, 5-7
- WebDAVDoNotSetTitleToOriginalName, 5-2
- Windows Explorer
 - and WebDAV security, 3-5
- workflows
 - WebDAV, 5-7

Z

zero-byte files, 5-5