Oracle® Universal Content Management

Folders and WebDAV Installation Guide

Release 10*g*R3

July 2008

ORACLE®

Folders and WebDAV Installation Guide, Release 10*g*R3 (10.1.3.3.3)

Primary Author: Ron van de Crommert

Contributing Author: Karen Johnson

Contributor: Mark Plotnick, Lyle Sitzman, Peter Walters

Contents

Index

Preface

This guide explains how to install and configure the Folders component and WebDAV. Folders is an optional component for use with Content Server that provides a hierarchical folder interface to content in Content Server in the form of "virtual folders" (also called "hierarchical folders"). 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.

Audience

This guide is intended for integrators and administrators of Oracle Content Server.

Documentation Accessibility

Our goal is to make Oracle products, services, and supporting documentation accessible, with good usability, to the disabled community. To that end, our documentation includes features that make information available to users of assistive technology. This documentation is available in HTML format, and contains markup to facilitate access by the disabled community. Accessibility standards will continue to evolve over time, and Oracle is actively engaged with other market-leading technology vendors to address technical obstacles so that our documentation can be accessible to all of our customers. For more information, visit the Oracle Accessibility Program Web site at http://www.oracle.com/accessibility/.

Accessibility of Code Examples in Documentation

Screen readers may not always correctly read the code examples in this document. The conventions for writing code require that closing braces should appear on an otherwise empty line; however, some screen readers may not always read a line of text that consists solely of a bracket or brace.

Accessibility of Links to External Web Sites in Documentation

This documentation may contain links to Web sites of other companies or organizations that Oracle does not own or control. Oracle neither evaluates nor makes any representations regarding the accessibility of these Web sites.

TTY Access to Oracle Support Services

Oracle provides dedicated Text Telephone (TTY) access to Oracle Support Services within the United States of America 24 hours a day, 7 days a week. For TTY support, call 800.446.2398. Outside the United States, call +1.407.458.2479.

Related Documents

For more information, see the following documents in the documentation set:

- *Content Server Folders and WebDAV Administration Guide*: This document provides system management and maintenance information for Folders and WebDAV.
- *Content Server Folders and WebDAV User Guide*: This document provides information to help content consumers and contributors work with Folders and WebDAV effectively.

Conventions

The following text conventions are used in this document:

Convention	Meaning
boldface	Boldface type indicates graphical user interface elements associated with an action, or terms defined in text or the glossary.
italic	Italic type indicates book titles, emphasis, or placeholder variables for which you supply particular values.
`monospace`	Monospace type indicates commands within a paragraph, URLs, code in examples, text that appears on the screen, or text that you enter.
Forward slashes (/)	Forward slashes are used to separate the directory levels in a path to a UNIX server, directory, or file. Forward slashes are also used to separate parts of an Internet address. A forward slash will always be included at the end of a UNIX directory name and might or might not be included at the end of an Internet address.
Backward slashes (\)	Backward slashes are used to separate the levels in a path to a Windows server, directory, or file. A backward slash will always be included at the end of a Windows server, directory, or file path.
<*Instance_Dir*>/	This notation refers to the location on your system of the main product installation directory.

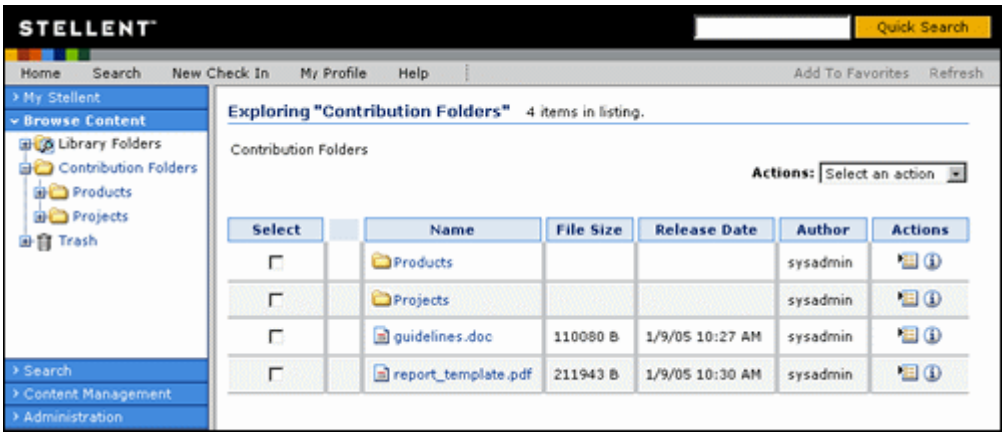
1 Introduction

This section covers the following topics:

1.1 About Folders

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

Figure 1–1 Virtual Folders in Content Server Interface



1.2 About WebDAV

WebDAV (Web-Based Distributed Authoring and Versioning) provides a way to remotely author and manage your 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 Content Server repository rather than using Oracle's web browser interface.

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

This section covers the following topics:

1.2.1 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. 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.

1.2.2 WebDAV Clients

A WebDAV client is an application that can send requests and receive responses using the WebDAV protocol. 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.

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 (Word, Excel, PowerPoint). This is not the same as Oracle WebDAV Client, which is a separate Oracle product that enhances the WebDAV interface to the content server.

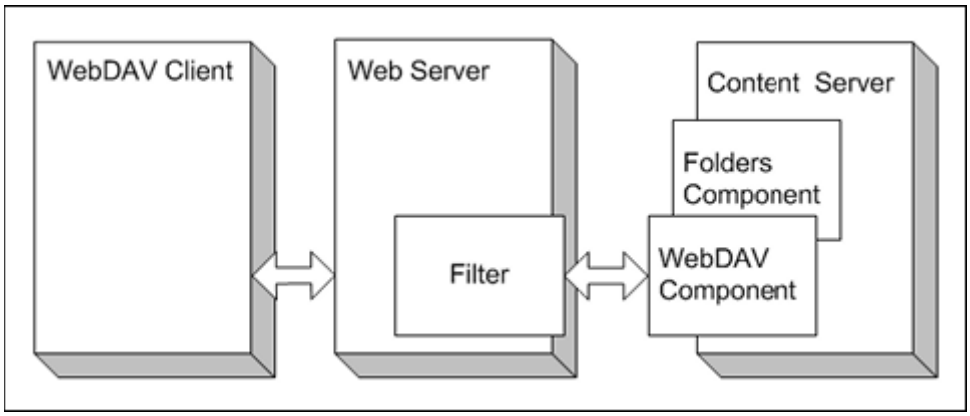
Note: Oracle offers the Desktop Integration Suite, which can enhance your WebDAV client environment by offering integrations into Windows Explorer, Microsoft Outlook, Lotus Notes, and other applications.

1.2.3 WebDAV Architecture

WebDAV support is implemented in the content server through a core component, called CoreWebDav, which handles WebDAV requests directly. A WebDAV request to the content server follows the following process as illustrated in Figure 1–2:

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 1–2 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.

1.2.4 Security

The following security features are included in WebDAV functionality:

- Access
- Read-Only Permission
- Login Cookie
- Windows Explorer
- Session Timeout

1.2.4.1 Access

The user logins and security controls in the Folders component and Oracle 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.

1.2.4.2 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.)

1.2.4.3 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/CoreWebDav/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/CoreWebDav/webdav_environment.cfg configuration file is used to generate the key.

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.

1.2.4.4 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.

1.2.4.5 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/CoreWebDav/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.

2

Pre-Installation Tasks and Considerations

This section covers the following topics:

2.1 Installation Requirements and Compatibilities for Folders

This section lists the software requirements and other compatibility issues for the Folders component

- In Content Server release 10gR3 (version 10.1.3.3.3) the Folders component is renamed the *Folders_g* component, and it is a separate component from WebDAV.
- The Folders_g component is ***not*** compatible with Content Server 7.1, 7.1.1, 7.51, or 7.5.2. For those older versions of Content Server, if you want to use Folders you must continue to use the legacy Folders component.
- The Folders_g component ***is*** compatible with earlier Content Server 10gR3 versions, but your Content Server installation must include the 10gR3CoreUpdate component (included in the 10gR3UpdateBundle), and you must restart the Content Server Admin Service after that component has been installed, as well as restart Content Server. Restarting the Admin Service enables the Folders_g installation to automatically disable the components belonging to the older Folders installation.
- If you are installing a new Content Server 10gR3, you can automatically install Folders_g during the Content Server installation, or you can manually install the component at another time.
- If you already have Folders installed on an earlier version of Content Server 10gR3, you can upgrade to Folders_g by installing the software as described in chapter 3 of this document.
- If you are upgrading from Content Server 7.x to Content Server 10gR3 (version 10.1.3.3.3) and you already have Folders installed, you need to upgrade the Folders component to Folders_g (which will disable all Folders 7.x components).
- The Document Folder Archiving component is no longer shipped with Content Server 10gR3 (vesion 10.1.3.3.3). Instead, the Folder Structure Archive component provides additional archive functionality.

  If you are upgrading from Content Server 7.x or from an earlier version of Content Server 10gR3, you can continue to use the Document Folder Archiving component. See the *Folders and WebDAV Installation Guide* for your earlier release

for information on retaining folder and content organization using the Document Folder Archiving component.

- The 10gR3 version of the Folders component also works with Collaboration Manager.

For more information on manually setting up Folders, see Chapter 3, "Installing Folders and WebDAV".

2.2 Installation Requirements for WebDAV

This section lists the software requirements and other installation prerequisites for providing WebDAV functionality:

- The CoreWebDav component must be installed and enabled for Content Server to provide WebDAV functionality. The CoreWebDav component is a standard system component in Content Server 10gR3 (version 10.1.3.3.3). It is enabled by default during Content Server installation.
- One of the following operating systems must be installed on the client machines:
  - Microsoft Windows 2000
  - Microsoft Windows XP (Home or Professional)
  - Microsoft Windows Server 2003
- At least one of the following must be installed on the client machines:
  - Microsoft Office 2000 (SP1 or later)
  - Microsoft Office XP
  - Microsoft Office 2003
  - Microsoft Internet Explorer 5.0 or greater with the Web Folders option enabled (this option is enabled during a "full" install of Internet Explorer)

Important: It is recommended that you install Microsoft Office to ensure that you get a working copy of Web Folders. The Web Folders software that ships with certain versions of Internet Explorer is known to corrupt WebDAV filenames under certain circumstances. In particular, Web Folders in Internet Explorer version 6.0.2800.1106 (SP1) truncates file names under certain circumstances.

- One or more WebDAV client applications must be installed on the client machines:
  - Microsoft Windows Explorer
  - Microsoft Word 2000, 2002 (XP), or 2003
  - Microsoft Excel 2000, 2002 (XP), or 2003
  - Microsoft PowerPoint 2000, 2002 (XP), or 2003

See "Setting Up WebDAV on Client Computers" on page 4-8 for more information.

Windows 95 and Windows 98 support WebDAV functionality through Windows Explorer if Internet Explorer 5.0 or greater is installed with the Web Folders option enabled. Versions of client applications earlier than Office 2000 and/or other browser versions may not work with these client operating systems.

Microsoft Office applications running on Mac OS X may not be WebDAV compliant. Specifically, Microsoft Office 2004 and Mac OS X 10.4.*x* do not work well with WebDAV.

2.3 Important Considerations for Folders

This section covers important installation considerations related to the Folders component:

- Limiting Number of Folders and Content Items
- Retaining Folder and Content Organization
- Backing Up Files Before Upgrading Folders
- Other Considerations

2.3.1 Limiting Number of Folders and Content Items

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. These numbers are initially set during the Folders/WebDAV software installation, but they can be modified afterwards (see the *Folders and WebDAV Administration Guide*).

To improve performance when browsing through folders, you can use set the `CollectionContentSecurity` and `CollectionFolderSecurity` parameters, which reduce security, but speed up browsing. You can also set the `CollectionDisplayResultSetSize` parameter, which limits the number of items and folders that are displayed on Exploring pages. See Appendix A, "Configuration Settings" for more information on these configuration parameters.

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.

2.3.2 Retaining Folder and Content Organization

It is recommended that the Folder Structure Archive component be used for archiving content within Folder structures. The Folder Structure Archive component enables document and folder organization to be maintained using the Archiver application.

The Folder Structure Archive component provides an alternative to using the Export Archive and Import Archive functions on the Virtual Folder Administration Configuration page. The two methods to archive a folder hierarchy and corresponding content items include:

- **Method 1**: Archiving a folder structure and content using Export/Import Archive functions in conjunction with the Archiver application.
- **Method 2**: Archiving a folder structure and content using the Folder Structure Archive component in conjunction with the Archiver application.

2.3.2.1 Export/Import Archive Functions Plus the Archiver Application

This method involves two basic steps. First, the folder structure is exported/imported using the Export/Import Archive functions, which removes all current folders from the target Content Server instance and replaces them with the imported hierarchy. Second, the content items are imported using the Archiver application.

The imported content items are sorted into their original folder locations. However, because the folder structure was removed from the target Content Server instance, any pre-existing content items must be manually moved to the new folders in the imported hierarchical structure.

The Export Archive function preserves the CollectionIDs between the source and target Content Server instances. Using this archival method does not forfeit Site Studio compatibility.

2.3.2.2 Folder Structure Archive Component Plus the Archiver Application

This method involves only one step because the Folder Structure Archive component functions automatically in combination with the Archiver application. When the Folder Structure Archive component is installed, the folder hierarchical structure is retained when content is imported using the Archiver application. This means that when content items are imported into the target Content Server, each content item is sorted into their original folder locations.

Also, it is not necessary to create the desired folder structure on the target Content Server instance before importing the content items. Instead, the Folder Structure Archive component automatically creates each folder, provided that the folder was selected for the folders archive. After the folder hierarchical structure is reproduced on the target Content Server, the imported content item files are placed into their original folder locations.

2.3.2.3 Issues and Considerations

Please note the following important considerations with regard to archiving and Folders:

- The Document Folder Archive component is no longer supported.
- You must select one of the two methods for replicating folder structures, because the Export/Import archive functions cannot be used in conjunction with the Folder Structure Archive component. Combining these functions may cause content items to be placed in the wrong folders.
- Both the source and target content server instances must have the Folder Structure Archive component installed to use the folder structure preservation option.
- If the folder structure is exported, all folders on the source content server instance are automatically created on the target content server instance (if they do not currently exist) after they are imported.

- When new folders are created on the target content server instance as a result of an archiving process, the custom folders metadata are retained from the original folders on the source content server instance.
- If the folder structure preservation option is not enabled during the Folders installation process and you subsequently want to use the functionality, you must manually install the Folder Structure Archive component. Either Component Wizard or Component Manager can be used for the manual installation process. The FolderStructureArchive.zip file is located in the Content Server install media /extras/ directory.

For further details on configuring virtual folders and archiving folders, see the *Folders and WebDAV Administration Guide* and the *Folder Structure Archive Administration Guide*.

2.3.3 Backing Up Files Before Upgrading Folders

All Folders parameters should be set in the folders_environment.cfg file located in the *[Instance_Dir]*/custom/ directory. Back up the folders_environment.cfg file before upgrading Folders, as this file is overwritten during installation. After Folders has been upgraded, merge your changes from the backed-up folders_environment.cfg file to the new file.

2.3.4 Other Considerations

Please note the following important considerations with regard to Folders:

- You cannot check two files with the same file name into the same folder (this limitation is required for WebDAV functionality).
- You must use the Folder Structure Archive component to archive content and folder structure from one Content Server to another Content Server.

3

Installing Folders and WebDAV

This section covers the following topics:

> **Caution:** The Microsoft URLScan ISAPI filter may prevent WebDAV from functioning properly. For this reason, it is recommended that the filter not be installed. If the filter is already installed, it should be disabled. For more information and disabling instructions, see "Disabling the URLScan ISAPI Filter" on page 4-1.

3.1 Upgrade and Reinstallation Considerations

In Content Server release 10gR3 (version 10.1.3.3.3) the Folders component is renamed the *Folders_g* component, and it is a separate component from WebDAV.

You can upgrade from an earlier version of Folders by installing the latest version on top of the existing instance. You do not need to uninstall or disable your existing Folders component prior to upgrading. If you are upgrading from an earlier Content Server 10gR3 release, you must upgrade to Folders_g (in Content Server release 10gR3 version 10.1.3.3.3).

The Folders_g component is compatible with earlier Content Server 10gR3 versions, but your Content Server installation must include the 10gR3CoreUpdate component (included in the 10gR3UpdateBundle), and you must restart the Content Server Admin Service after that component has been installed, as well as restart Content Server. Restarting the Admin Service enables the Folders_g installation to automatically disable the components belonging to the older Folders installation.

If you upgrade or reinstall Folders/WebDAV, the installation options (see "Installation Settings" on page 3-4) are set in accordance with the selected options of the previous installation. In addition, all existing configuration settings will be preserved.

Please note the following important considerations with regard to upgrading or reinstalling Folders and WebDAV:

3.1.1 Backing Up Configuration File Before Upgrading

All Folders parameters should be set in the folders_environment.cfg file located in the <*Installation_Dir*>/<*Instance_Dir*>/custom/ directory. Make sure that you back up the folders_environment.cfg file before upgrading Folders, as this file is overwritten during installation. After Folders has been upgraded, merge your changes from the backed-up folders_environment.cfg file to the new file.

3.1.2 Initial Folder ID

During the installation of the Folders software, you can specify the initial folder identifier for the server. When you reinstall or upgrade Folders, the existing initial folder identifier remains in effect, even if you specified a different value during the software upgrade or reinstallation. This is because when Folders is first installed, it creates the tables along with folders starting with the ID that was specified at that time. To use new IDs, you need to delete the tables created by Folders and also delete the collection ID counter in the Counters table. For further details, see "Manual Uninstallation" on page C-2 (specifically, steps 3, 4, and 7).

3.2 Installing the Folders Software

If you did not choose to automatically install Folders during a new Content Server 10gR3 installation, you can install the Folders component in either of two ways:

- Using Component Manager
- Using Component Wizard

3.2.1 Using Component Manager

Important: If you are installing the Folders component on a Collaboration Manager instance, you ***must*** select the recommended collaboration settings for the component to work properly. See the *Collaboration Manager Installation Guide* for the specific settings.

To install the Folders and WebDAV software using Component Manager, complete the following steps:

1. Make sure the Content Server software is installed and functioning properly.
2. Log into the content server as an administrator.
3. Go to the administration applets page of the content server, and click **Admin Server**.

   The Administration for Servers page is displayed.
4. Click on the appropriate server button.

   The options and status page of the content server instance is displayed.
5. Click **Component Manager** in the menu on the left.

   The Component Manager page is displayed.
6. Click **Browse** next to the Install New Component field.

   A file selection dialog is displayed.
7. Select the Folders_g.zip component file and close the file selection dialog.

8. Click **Install**.

   A page is displayed listing what will be installed.

9. Click **Continue**.

   The Install Settings page is displayed.

10. Modify the installation settings to suit your needs (see Table 3.4, "Installation Settings"), and click **Continue** when you are done.

11. Click **Continue** when you are done.

    All required files are now installed. After this process is completed, a page is displayed stating that the component was uploaded and installed successfully. You can then enable the component and restart the content server or return to the Component Manager page.

12. You ***must*** enable the component and restart the content server for everything to work correctly.

Depending on the content server environment and selected Folders options, you may need to perform some tasks after the Folders software installation. For details see Chapter 4, "Post-Installation Tasks and Considerations".

3.2.2 Using Component Wizard

Important: If you are installing the Folders component on a Collaboration Manager instance, you ***must*** select the recommended collaboration settings for the component to work properly. See the *Collaboration Manager Installation Guide* for the specific settings.

To install the Folders and WebDAV software using Component Wizard complete the following steps:

1. Make sure the Oracle Content Server software is installed and functioning properly.

2. Start Component Wizard:

   Windows: From **Start**, select **Programs**, then select **Stellent Content Server**. From ***<Instance_Name>***, select **Utilities**, then select **Component Wizard**.

   UNIX: Run the Component_Wizard script, located in the /bin subdirectory of the Folders and WebDAV installation directory.

3. Component Wizard is started, with the Component List dialog active.

4. Click **Install**.

   The Install dialog is displayed.

5. Click **Select**.

   A file selection dialog is displayed.

6. Select the Folders_g.zip component file and close the file selection dialog.

   The Install dialog now contains all files that will be installed.

7. Click **OK**.

   The Edit Preference Prompt dialog is displayed.

8. Modify the installation settings to suit your needs (see "Installation Settings" on page 3-4), and click **OK** when you are done.
9. Click **OK** when you are done.

   All required files are now installed. After this process is completed, a message is displayed asking whether the specified components should be enabled.
10. Click **Yes**.

    The component is now loaded and enabled. The main Component Wizard window now shows a list of the component resources.
11. Close Component Wizard. Restart the Content Server.
12. If you stopped the web server before installation, restart the web server.

Depending on the content server environment and selected Folders options, you may need to perform some tasks after the Folders software installation. For details see Chapter 4, "Post-Installation Tasks and Considerations".

3.3 Installing WebDAV

In Content Server release 10gR3 (version 10.1.3.3.3), WebDAV functionality is supported by the CoreWebDav component, which is automatically installed during Content Server installation.

3.4 Installation Settings

For more details on the various installation settings and configuration variables, see Appendix A, "Configuration Settings".

During the installation process, you are prompted to specify the following settings:

- Choose whether you want users to be able to download content items for which they have Read permission (R).
  - Recommended: Accept the default (enabled).
  - Optional: Disable the selection.

  See "CollectionReadOnlyMeta" on page A-5 for details.
- Choose whether you want users to be able to specify whether a virtual folder and its contents are hidden or visible. To enable, accept the default (xHidden) or enter a different field name.
  - Recommended: Accept the default (xHidden).
  - Optional: Delete the default information field and leave the entry blank.

  See "CollectionHiddenMeta" on page A-4 for further details (including instructions on how to manually disable this functionality again).
- Choose whether you want users to be able to specify whether a virtual folder and its contents are read-only. To enable, accept the default (xReadOnly) or enter a different field name. The read-only feature is subject to certain idiosyncrasies of various client environments. Therefore, not all clients will honor the read-only flag.
  - Recommended: Accept the default (xReadOnly).
  - Optional: Delete the default information field and leave the entry blank.

See "CollectionReadOnlyMeta" on page A-5 for further details (including instructions on how to manually disable this functionality again).

- Choose whether you want users to be able to move folders and content items to other folders. This displays/hides the option on the web interface.
  - Recommended: Accept the default (enabled).
  - Optional: Disable the selection.

  See "CollectionMoveEnabled" on page A-7 for further details.
- Choose whether users can delete folders and content items. This displays/hides the option on the web interface.
  - Recommended: Accept the default (enabled).
  - Optional: Disable the selection.

  See "CollectionDeleteEnabled" on page A-7 for further details.
- Enter the name of an inhibit field for the metadata propagation function.
  - Recommended: Accept the default (xInhibitUpdate).
  - Optional: Enter a different field name.

  See "CollectionInhibitUpdateMeta" on page A-8 for further details.
- Choose whether users can force folder security on Folder content.
  - Recommended: Accept the default (enabled).
  - Optional: Disable the selection.

  See CollectionForceFolderSecurityEnabled for further details.
- Choose the field name used to determine a folder's Force Folder Security status.
  - Recommended: Accept the default (xForceFolderSecurity).
  - Optional: Enter a different field name.

  See CollectionForceFolderSecurityMeta for further details.
- Choose whether to enable the optional Trash Bin settings.
  - Selecting this option enables the following Trash Bin settings:
    * CollectionTrashDeleter
    * CollectionTrashDeleteDate
    * CollectionTrashDeleteLocation
    * CollectionTrashDeleteOldName
  - If you do not want to enable the optional Trash Bin settings, clear the check box (this option is enabled by default). Enabling this selection enables ***all*** of the above optional settings.
- If using WebDAV, specify the key used to encrypt the WebDAV cookie to avoid spoofing and replay attacks.
  - Recommended: Enter an encryption key.
  - Optional: Accept the default.

  See "WebDAVSecretKey" on page A-18 for details.

- Enter the maximum number of folders per virtual folder.
  - Recommended: Accept the default.
  - Optional: Enter a new number.

  If more than 1,000 subfolders per virtual folder are allowed, content server performance and request times may be affected. In addition, it makes it harder for users to find items in folders since they need to browse through very large lists. For more information on limiting the number of folders per virtual folder, see the *Folders and WebDAV Administration Guide*.
- Enter the maximum number of content items per virtual folder.
  - Recommended: Accept the default.
  - Optional: Enter a new number.

  If more than 1,000 content items per virtual folder are allowed, content server performance and request times may be affected. In addition, it makes it harder for users to find items in folders since they need to browse through very large lists. For more information on limiting the number of content items per virtual folder, see the *Folders and WebDAV Administration Guide*.
- Enter the initial folder identifier for this server. (The number entered is pre-calculated in millions. For example, 0 = 0000000.)
  - Recommended: Accept the default of 0.
  - Optional: Enter a new number.

  See "InitialColID" on page A-13 for further details.

3.5 Rebuilding the Collection

The term *collection* is used to refer to a particular content server folder and the content within that folder. A *folder collection* is not the same as an *archive collection*.

During the installation process, Folders adds some metadata fields to the search page (such as Hidden and Read Only) which can be used as possible search criteria. If you want to use any of the new fields as search criteria, you need to rebuild the collection. Otherwise, attempting to do a search before rebuilding the collection will return no results. For more detailed information about the additional metadata fields, see Appendix B, "Installation Details".

To rebuild the collection, complete the following steps:

1. Log into the content server as an administrator.
2. On the Administration page of the content server instance, click **Repository Manager**.

   The Repository Manager window is displayed.
3. Open the **Indexer** tab.
4. On the Collection Rebuild Cycle pane, click **Start**.

4

Post-Installation Tasks and Considerations

Depending on the content server environment and the options selected during the Folders/WebDAV software installation, you may need to perform a number of post-installation tasks:

- Disabling the URLScan ISAPI Filter
- Manually Setting Up the Trash Folder
- Configuring WebDAV in the Web Server
- Configuring WebDAV on the Content Server
- Setting Up WebDAV on Client Computers
- Implementation Considerations for WebDAV

4.1 Disabling the URLScan ISAPI Filter

URLScan is available for download from the Microsoft web site. However, providing comprehensive documentation for the proper configuration and compatibility testing is beyond the scope of this guide. Detailed instructions for installing and using the filter are available in the URLScan download package.

The Microsoft URLScan ISAPI filter allows web server administrators to ensure the security of their servers. URLScan screens all incoming requests to the server and filters them based on rules established by the administrator. Server security is enhanced because the filtering process helps ensure that the server only responds to valid requests.

URLScan provides security by restricting the types of HTTP requests that IIS will process. By default, it blocks certain WebDAV methods such as PROPFIND, PROPPATCH, MKCOL, DELETE, PUT, COPY, MOVE, LOCK, UNLOCK, OPTIONS, and SEARCH. If these methods are blocked, WebDAV will not work. However, URLScan can be configured to allow these methods as well as necessary headings (Translate:, If:, and Lock-Token:).

Important: The URLScan filter may cause WebDAV used with Content Server to fail. URLScan can only be used at the server level, which means that this is a global tool that applies to every web site defined in IIS. This means that if you configure URLScan to allow the WebDAV methods to pass through, these methods and headers will be allowed to pass through to every website, not just the Oracle website. For more detailed information, see the available Microsoft Knowledge Base articles specifically related to URLScan.

If the URLScan ISAPI filter is not properly configured to be compatible with Oracle software, it may prevent WebDAV from functioning properly. For this reason, it is recommended that the filter not be installed. If the filter is already installed, it should be disabled.

To disable URLScan, complete the following steps:

1. Stop all the content server services (names starting with "IDC").
2. From the **Start** menu, select **Programs**, **Administrative Tools**, then select **Internet Services Manager** to open the IIS Admin window.
3. Double-click the server.
4. Right-click **Default Web Site** and select **Properties**.

   The Default Web Site Properties window is displayed.
5. Open the **ISAPI Filters** tab.
6. Select the UrlScan filter and click **Remove**.
7. Click **OK**.
8. Restart all content server services (names starting with "IDC").
9. Restart the IIS Admin Service.

4.2 Manually Setting Up the Trash Folder

If the Folders component was previously installed on the content server and the associated database tables still exist, you need to create the Trash folder manually. This step is not required for a new installation or if you will not be using the optional Trash Bin function:

1. Start your web browser.
2. Enter the following command in the web browser address bar:

   ```
   http://<web_server_name>/<web_root>/idcplg/webdav?
   IdcService=COLLECTION_ADD
   &dCollectionName=Trash
   &dParentCollectionID=-1
   &hasParentCollectionID=true
   &force=true
   &hasMark=true
   &mark=TRASH
   ```

   This entire command should be provided as a single string.
3. When prompted to log in, provide the correct administrator username and password.
4. Click the **Folders** link to display the System-Level Exploring page.

   The Trash folder should be displayed along with the Contribution Folders folder.

4.3 Configuring WebDAV in the Web Server

If you chose to enable the WebDAV features during the Folders installation, you need to set up WebDAV in the web server:

- Configuring WebDAV on iPlanet/Sun ONE (Windows)
- Configuring WebDAV on iPlanet/Sun ONE (UNIX)

- Configuring WebDAV on IIS
- Using a WebDAV Folder in IIS to Test Web Folders

4.3.1 Configuring WebDAV on iPlanet/Sun ONE (Windows)

If you are using an iPlanet/Sun ONE web server on Microsoft Windows, you must configure the web server to allow WebDAV requests as follows:

1. Edit the web server's access control list (ACL).
   a. Open the ACL file in a text editor. (For example, *C:\iPlanet\Servers\httpacl\generated\.https-myserver.acl*.)
   b. Add the following two lines:

```
acl "stellentacl";
allow (read, list, execute, info, write, delete) user = "anyone";
```

   c. Save and close the ACL file.
2. Edit the web server's Init parameters.
   a. **iPlanet/Sun ONE 6.0 and later:** Open the magnus.conf file in a text editor.
   b. **iPlanet pre-6.0:** Open the obj.conf file in a text editor.
   c. Add the following new Init parameters:

```
Init fn="register-http-method"
methods="OPTIONS,PROPFIND,COPY,DELETE,LOCK,MKCOL,MOVE,PROPPATCH,PUT,UNLOCK"
```

   d. Save and close the magnus.conf or obj.conf file.
3. Edit the web server's obj.conf file.
   a. Open the obj.conf file in a text editor.
   b. In the `default` object, add the `name` parameter to the NameTrans line that points to the /weblayout directory. This changes the redirect to use the newly defined ACL object:

```
<Object name="default">
NameTrans fn="pfx2dir" from="<web_root>" dir="[Instance_Dir]/weblayout"
name="stellentaclobject"
</Object>
```

   c. Create a new object and include the lines shown below. This defines an ACL object that supports DAV methods:

```
<Object name="stellentaclobject">
PathCheck fn="check-acl" acl="stellentacl"
</Object>
```

   d. Define the `stellent` ACL path to support WebDAV methods by modifying the following object in the obj.conf file:

```
<Object ppath="[Instance_Dir]/weblayout/*">
NameTrans fn="idcNameTrans"
PathCheck fn="idcPathCheck"
Service
method="(GET|HEAD|POST|OPTIONS|PROPFIND|COPY|DELETE|LOCK|MKCOL|MOVE|PROPPAT
CH|PUT|UNLOCK)" fn="idcService"
</Object>
```

If you are already using iPlanet, the first three lines in the above object will already exist. The fourth line (`Service method=`) will need to be added.

e. Save and close the obj.conf file.

4. Restart the web server.

4.3.2 Configuring WebDAV on iPlanet/Sun ONE (UNIX)

If you are using an iPlanet/Sun ONE web server on UNIX, you must configure the web server to allow WebDAV requests as follows:

1. Edit the web server's access control list (ACL).
   a. Open the ACL file in a text editor. (For example, *//iPlanet_ubstall_dir]/Servers/httpacl/generated.https-myserver.acl*.)
   b. Add the following two lines:

```
acl "stellentacl";
allow (read, list, execute, info, write, delete) user = "anyone";
```

   c. Save and close the ACL file.
2. Edit the web server's Init parameters.
   a. **iPlanet/Sun ONE 6.0 and later:** Open the magnus.conf file in a text editor.

      iPlanet pre-6.0: Open the obj.conf file in a text editor.
   b. Add the following new Init parameters:

```
Init fn="register-http-method"
methods="OPTIONS,PROPFIND,COPY,DELETE,LOCK,MKCOL,MOVE,PROPPATCH,PUT,UNLOCK"
```

   c. Save and close the magnus.conf or obj.conf file.
3. Edit the web server's obj.conf file.
   a. Open the obj.conf file in a text editor.
   b. In the default `object`, add the `name` parameter to the NameTrans line that points to the Oracle /weblayout directory. This changes the redirect to use the newly defined ACL object:

```
<Object name="default">
NameTrans fn="pfx2dir" from="<web_root>" dir="[Instance_Dir]/weblayout"
name="stellentaclobject"
</Object>
```

   c. Create a new object and include the lines shown below. This defines an ACL object that supports DAV methods:

```
<Object name="stellentaclobject">
PathCheck fn="check-acl" acl="stellentacl"
</Object>
```

d. Define the `stellent` ACL path to support WebDAV methods by modifying the following object in the obj.conf file:

```
<Object ppath="[Instance_Dir]/weblayout/*">
NameTrans fn="idcNameTrans"
PathCheck fn="idcPathCheck"
Service
method="(GET|HEAD|POST|OPTIONS|PROPFIND|COPY|DELETE|LOCK|MKCOL|MOVE|PROPPAT
CH|PUT|UNLOCK)" fn="idcService"
</Object>
```

If you are already using iPlanet, the first three lines in the above object will already exist. the fourth line (`Service method=`) will need to be added.

e. Save and close the obj.conf file.

4. Restart the web server.

4.3.3 Configuring WebDAV on IIS

If any client machines will be using Microsoft Office XP applications to interact with the content server through WebDAV, you must set Read permission on the web filter virtual directory. This procedure is not required if no Office XP applications are being used as WebDAV clients.

1. Open the Internet Information Services screen (typically from **Start**, select **Programs**, then **Administrative Tools**, then select **Internet Services Manager**).
2. Expand the tree for the computer where the web server is located.
3. Expand the tree for the **Default Web Site**.
4. Select the name of the content server instance assigned during Content Server installation.
5. Right-click the **idcplg** directory, and select **Properties**.
6. Under **Local Path**, select the **Read** check box.
7. Click **OK**.
8. Close the Internet Information Services screen.

4.3.4 Using a WebDAV Folder in IIS to Test Web Folders

If you are experiencing difficulty creating a web folder to connect to your content server through WebDAV, you can, instead, create a WebDAV folder in IIS to test the functionality outside of Content Server. Doing so will help determine if your web folders work correctly when the content server is not involved.

Testing web folders and IIS involves the following steps:

- Setting Up the WebDAV Directory
- Enabling Anonymous User Access
- Testing the New WebDAV Folder

4.3.4.1 Setting Up the WebDAV Directory

To set up the WebDAV directory, complete the following steps:

1. Create a new folder inside your C:\inetpub folder. For example, *WebDAV_test* is good for identification purposes. This folder can be located anywhere except

inside your \inetpub\wwwroot\ folder, because its default DACLs (Discretionary Access Control Lists) are different from those on other directories. See the IIS documentation for more information.

2. In the IIS snap-in for the Microsoft Management Console (MMC), create a virtual directory:
   a. Right-click on the Default Web Site.
   b. Select **New**, then select **Virtual Directory**.
   c. Enter **`WebDAV_test`** as the alias for the virtual directory.
   d. Link the alias to the physical directory you created in Step 1.
3. Make sure Directory Browsing is selected, and grant Read, Write, Script and Browsing access.

   The folder can now be accessed via the WebDAV protocol. Once your WebDAV directory is set up, users with the correct permissions can read and write to this directory.

4.3.4.2 Enabling Anonymous User Access

To enable anonymous user access, complete the following steps:

1. Select the Directory Security Tab in the properties dialog for the directory created previously.
2. Click the **Edit** button in the Anonymous Access and Authentication Controls box.
3. In the Authentication Methods dialog, enable the **Anonymous access** setting for the directory.

Another more restrictive approach to user access would be to authenticate specific users by creating valid Windows user accounts and then configure the Windows file system (NTFS) directory and file permissions for those accounts.

> **Important:** Because support for WebDAV is integrated with Windows and IIS, it requires understanding aspects of the Windows operating systems in addition to IIS. See the IIS documentation for more information about available security options.

4.3.4.3 Testing the New WebDAV Folder

To test the new WebDAV folder, complete the following steps:

1. In an Internet Explorer browser window, from the **File** menu, select **Open**.
2. Browse for the WebDAV folder's URL or enter it in the Open field.

   For example, http://<*server_name*>/WebDAV_test
3. Select the **Open as Web Folder** check box.
4. Click **OK**.

You can also test the new WebDAV folder by using the same URL to add a network place in Network Neighborhood.

You should be able to view, move, and copy files into and out of the browser window as if it were in Windows Explorer.

When you create a WebDAV accessible folder, there are important security issues that must be considered. In the above test scenario, a WebDAV folder was set up without

regard for the security of the website. However, for a production website, you should make sure your implementation meets the security standards established by your organization.

4.4 Configuring WebDAV on the Content Server

This section covers the following topics:

4.4.1 Setting the WebDAV Secret Key

If you want to use WebDAV, you need to change the default value of the WebDAV secret key. This key is used to encrypt WebDAV login cookies on the local content server instance. Each content server should have a unique value to prevent login cookies that are generated on one content server instance from being used on any other content server.

To change the WebDAV secret key, complete the following steps:

1. Open the *[Instance_Dir]*/custom/CoreWebdav/webdav_environment.cfg configuration file in a text editor.
2. Change the value of the `WebDAVSecretKey` parameter to any unique string.
3. Save and close the file.
4. Restart the content server.

4.4.2 Using WebDAV with the ExtranetLook Component

WebDAV uses CookieLoginPlugin.dll for cookie-based login. The cookies eliminate additional login prompts when Microsoft Word opens a document using WebDAV. Typically, the implementation keeps the dll file from doing forms-based logins on a web page because most users do not want this. However, if users do want forms-based logins, you can enable this by making a WebDAV configuration change:

1. Open the *[Instance_Dir]*/custom/CoreWebdav/webdav_environment.cfg configuration file in a text editor.
2. Set the `WebDAVDisableOtherFilterCookies` parameter to 'false' ('true' is the default):

   ```
   WebDAVDisableOtherFilterCookies=false
   ```

3. Save and close the file.
4. Restart the content server.

This allows you to use WebDAV along with the ExtranetLook component. See Appendix A, "Configuration Settings" for more information on the parameter.

4.4.3 "Reuse Revision" Setting

By default, a new revision is created only when an open WebDAV document is saved and closed. This "reuse revision" feature is recommended for environments where frequent file saves can result in a large number of unnecessary revisions, such as when users save their files often while they are working, or when the "auto-save" feature is

enabled in WebDAV clients such as Microsoft Word. The "reuse revision" feature is implemented by two settings:

- The Folders component installer automatically enables the "Allow author to delete revision" content server setting, which ensures that the last revision can be deleted and a new revision created each time an open document is saved in a WebDAV folder.
- By default, the `WebDAVReuseRevision` parameter is set to *true* in the *[Instance_Dir]*/custom/CoreWebdav/webdav_environment.cfg configuration file. See "WebDAVReuseRevision" on page A-18 for further details.

If you want each save (including auto-saves) to create a new revision, you can disable the reuse revision feature as follows:

1. Log into the content server as an administrator.
2. Open the Admin Server page.
3. Click on the button of the appropriate content server instance.

   The configuration page for the content server instance is displayed.
4. Click on **Content Security** in the menu on the left.
5. Clear the **"**Allow author to delete revision" check box.
6. Click **Save**.
7. Open the *[Instance_Dir]*/custom/CoreWebdav/webdav_environment.cfg configuration file in a text editor.
8. Set the `WebDAVReuseRevision` parameter to 'false':

   ```
   WebDAVReuseRevision=false
   ```
9. Save and close the file.
10. Restart the content server.

4.5 Setting Up WebDAV on Client Computers

Use the following procedure to set up the WebDAV interface to Content Server on a client computer:

1. Install one or more WebDAV client applications:
   - Microsoft Windows Explorer
   - Microsoft Word 2000, 2002 (XP), or 2003
   - Microsoft Excel 2000, 2002 (XP), or 2003
   - Microsoft PowerPoint 2000, 2002 (XP), or 2003

   Make sure that you use Microsoft Office 2000 SP1 or later.
2. Make sure that Microsoft Internet Explorer 5.0 or greater is installed, with the Web Folders option enabled during installation.
3. To be able to access Oracle pages though Windows Explorer, make sure that Internet Explorer 5.5 or 6.0, or Office 2000 or later is installed.
4. For clients that use Internet Explorer, make sure that the browser is not using a proxy server. See "Configuring Third-Party Products" on page 4-10 for more information.

5. Set up web folders on the client machine:
   a. In Windows Explorer, click **My Network Places** in the left pane (Folders list).
   b. Double-click **Add Network Place** in the right pane.

      The Add Network Place Wizard screen is displayed.
   c. Enter the web address of the WebDAV component. For example:

      On a master content server:

      ```
      http://my_computer/stellent/idcplg/webdav
      ```

      On a proxy content server:

      ```
      http://my_computer/stellent/idcplg/stellent_2/pxs/webdav
      ```

      In these examples, *my_computer* is the web server name, and *stellent_2* is the relative web root of the proxied content server.
   d. Click **Next**. You are prompted for a network password.
   e. Enter your Oracle user name and password, and click **OK**.
   f. Enter a name for the top level virtual folder.
   g. Click **Finish**.

   You should now be able to access the virtual folders through My Network Places.
6. For machines that are running client applications on Windows Server 2003, enable the WebClient service:
   a. From the **Start** menu, select **Programs**, then **Administrative Tools**, and then select **Services**.

      The Services screen is displayed.
   b. Right-click on the WebClient service and select **Properties**.

      The WebClient Properties screen is displayed.
   c. In the **Startup type** list, select **Automatic**.
   d. Under **Service status**, click **Start**.

      The WebClient service starts.
   e. Click **OK**.
7. Set the default metadata values for the user.
   - **Required:** Follow the steps listed in the Defining User Metadata Defaults for New Content section of the *Folders and WebDAV User Guide*.
   - **Optional:** Follow the steps listed in the Defining User Metadata Defaults for Revised Content section of the *Folders and WebDAV User Guide*.

     User default metadata values should also be set for each user after a required field is added to the content server or after accounts are enabled.

4.6 Implementation Considerations for WebDAV

The following special considerations should be taken into account when implementing WebDAV functionality with Content Server:

- Configuring Third-Party Products

4.6.1 Configuring Third-Party Products

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 may need to reconfigure them to allow the WebDAV methods.

In addition, because of these HTTP method limitations, a client machine cannot connect to a WebDAV server from Windows Explorer if Internet Explorer is configured to use a proxy server. (In Internet Explorer, from **Tools**, select **Internet Options**, **Connections**, then select **LAN Settings**. Then see if the **Use a Proxy Server** check box is selected.) There are two ways to resolve this problem:

- You can configure client machines to not use the proxy server instance for your web server. To do this in Internet Explorer 5.0 or greater, from **Tools**, select **Internet Options**, then **Connections**, then **LAN Settings**. Then from **Advanced**, select **Exceptions** and specify the IP address/host name of the web 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. See your proxy server documentation for more information.

A

Configuration Settings

This section covers the following topics:

A.1 Folders Configuration Files

The Folders component derives its configuration settings from the following configuration files:

- [*Instance_Dir*]/data/components/Folders/config.cfg
- [*Instance_Dir*]/data/components/Folders/install.cfg
- [*Instance_Dir*]/custom/Folders/folders_environment.cfg

Content Server loads these configuration files sequentially in the order listed above. This means that if a variable is set in more than one of these files, the value set in *[Instance_Dir]*/config/config.cfg takes precedence over all others.

Even though you can set most Folders configuration parameters in *[Instance_Dir]*/config/config.cfg, it is strongly recommended that you set all parameters in *[Instance_Dir]*/custom/folders/folders_environment.cfg, unless specifically stated otherwise. This allows disabling or uninstalling the Folders component to remove its entries automatically without forcing the administrator to look through other configuration and environment files on the server to delete the Folders-related entries manually.

The folders_environment.cfg file should be backed up before performing an update install. After the update, the changes to this file should be merged back in to the new folders_environment.cfg file that is installed during the update.

During the Folders installation, you may not have selected the default installation settings. Also, you may have made additional changes to the Folders installation. If that is the case, you should make sure that you back up the [*Instance_Dir*]/custom/folders/folders_environment.cfg file before performing an upgrade. Otherwise, your Folders configuration file is overwritten during the upgrade process.

A.2 Setting Variables during Folders Installation

During the Folders software installation process, you are prompted to specify the initial values of a number of configuration settings (see "Installation Settings" on page 3-4 for details). You can accept the suggested defaults, or make changes as required. The specified settings are stored in the Folders configuration files (see "Folders Configuration Files" on page A-1 for details) and remain valid until they are changed, either using Component Manager (see below) or directly in the configuration files (not recommended).

A.3 Editing Variables Using Component Manager

To change the value of a configuration variable, the preferred method is to use Component Manager. Not all of the configuration variables documented in this appendix can be edited using Component Manager. If the configuration variable that you want to edit is not listed in Component Manager, you need to edit it directly in the configuration file (for example, folders_environment.cfg).

1. Log into the content server as an administrator.
2. Go to the administration applets page of the content server, and click **Admin Server**.

   The Administration for Servers page is displayed.
3. Click on the appropriate server button.

   The options and status page of the content server instance is displayed.
4. Click **Component Manager** in the menu on the left.

   The Component Manager page is displayed.
5. In the Update Component Configuration field, select **Folders** from the option list.
6. Click **Update**.

   The Update Component Configuration page is displayed.
7. Make the desired changes to the applicable configuration variables. See "Configuration Variables for Folders" on page A-2 for a detailed description of each configuration variable.
8. Click **Update** when you are done.

   A page is displayed stating that the configuration was updated successfully.
9. Click the link to return to the Component Manager page.

Important: If you modify any configuration settings, you ***must*** restart the content server to apply the changes.

A.4 Configuration Variables for Folders

The following configuration variables are available for Folders:

- CollectionMeta
- CollectionHiddenMeta
- CollectionReadOnlyMeta
- CollectionSecurityReadOnly

- CollectionMoveEnabled
- CollectionDeleteEnabled
- CollectionWebDAVServer
- CollectionInhibitUpdateMeta
- CollectionForceFolderSecurityEnabled
- CollectionForceFolderSecurityMeta
- CollectionTrashDeleter
- CollectionTrashDeleteDate
- CollectionTrashDeleteLocation
- CollectionTrashDeleteOldName
- FolderToTrashDeleteAccessIsStrict
- CollectionReadOnlyMarkedFolders
- InitialColID
- CollectionReleasedOnly
- CollectionContentSecurity
- CollectionFolderSecurity
- CollectionUseCache
- CollectionDisplayResultSetSize
- CollectionPropagateEmptyValues
- CollectionMoveEnabled:actionPopup
- MaxHeadlineTableRows
- CollectionSearchRecursiveContent
- CollectionMaxBranch

Even though you can set most Folders configuration parameters in [*Instance_Dir*]/config/config.cfg, it is strongly recommended that you set all parameters in [*Instance_Dir*]/custom/folders/folders_environment.cfg, unless specifically stated otherwise. This allows disabling or uninstalling the Folders component to remove its entries automatically without forcing the administrator to look through other configuration and environment files on the server to delete the Folders-related entries manually.

Important: If you modify any configuration settings, you must restart the content server to apply the changes.

A.4.1 CollectionMeta

The **CollectionMeta** setting specifies the metadata field that is used to store the unique Collection ID for each virtual folder.

- The parameter format is `CollectionMeta=`*xField_Name*.
- If this setting is not specified in the configuration file, the default value for *xField_Name* is `xCollectionID`. Conversely, if your custom metadata field is named *CollectionID*, the *CollectionMeta* setting is not required in the configuration file.

- This variable is set automatically by the Folders installer program, according to the field name you enter.

A.4.2 CollectionHiddenMeta

The **CollectionHiddenMeta** setting enables users to specify whether a virtual folder and its content are hidden or visible.

- This setting adds Hide/Unhide icons to the Exploring pages. See Figure A–1 and Figure A–2.
- This setting adds a "Show hidden when browsing" check box to the Folder Configuration page.
- This variable is set automatically by the Folders installer program, according to the option you select.
- A new metadata field is added to the database.
- If you are using Content Server's default layout (headline view), enabling these values will not present a problem. However, if you are using the classic view, then the icons associated with this configuration variable are visible on the Exploring page.
- If enabled during the Folders installation, this variable must be manually disabled.

Figure A–1 Visible Icon

Figure A–2 Hidden Icon

A.4.2.1 Manually Enabling CollectionHiddenMeta

To enable the Hide/Unhide feature manually, complete the following steps:

1. Create a custom metadata field using Configuration Manager with the following parameters:
   - **Name =** Hidden
   - **Field Caption =** Hidden
   - **Field Type =** Text
   - **Enable on User Interface =** Selected
   - **Enable Option List =** Selected
   - **Option list values =** false and true

   Make sure that you update the database design in Configuration Manager to include the new field in your database. It is not necessary to rebuild your search index.
2. Add the following line to the Folders configuration file:

   ```
   CollectionHiddenMeta=xHidden
   ```

   You can name this field something other than Hidden, but the setting in the content server configuration file must match the field name. For example, if you name the field *Hide*, then `CollectionHiddenMeta=xHide`.

A.4.2.2 Manually Disabling CollectionHiddenMeta

To disable the Hide/Unhide feature manually, complete the following steps:

1. In a text editor, open each of the following configuration files (this variable may be set in more than one file):
   - [*Instance_Dir*]/data/components/Folders/config.cfg (not for CS 6.2)
   - [*Instance_Dir*]/data/components/Folders/install.cfg
   - [*Instance_Dir*]/custom/Folders/folders_environment.cfg
   - [*Instance_Dir*]/config/config.cfg
2. Comment out the `CollectionHiddenMeta` configuration variable, if it exists, by preceding its line with a hash symbol (#).
3. Save and close the edited configuration files.

Make sure that you comment out the configuration variable. Simply editing the variable in the configuration files by deleting or changing the metadata field value will not reverse the functionality nor will it remove the Hide/Unhide icons or Hidden metadata field from the user interface.

Commenting out the parameter line in the configuration file does not remove the Hidden metadata field from the database. If you want to clean up your database in regards to functionality that is not enabled, you may choose to remove the Hidden metadata field from the database. Please note that this requires the database design to be updated and the index rebuilt, which may take a considerable amount of time.

A.4.3 CollectionReadOnlyMeta

The **CollectionReadOnlyMeta** setting enables users to specify whether a virtual folder and its contents are read-only.

- "Read-only" means that you cannot rename, move, or delete the virtual folder or content items in that folder. You can still check in content and update metadata for read-only folders.
- The read-only feature is subject to certain idiosyncrasies of various client environments. Therefore, not all clients will honor the read-only flag.
- This setting adds Read-Only/Editable icons to the Exploring pages. See Figure A–3 and Figure A–4.
- This setting applies only to the current folder level. A subfolder does not inherit read-only status from its parent folder.
- This variable is set automatically by the Folders installer program, according to the option you select.
- This variable adds a new metadata field in database
- If you are using Content Server's default layout (headline view), enabling these values will not present a problem. However, if you are using the classic view, then the icons associated with this configuration variable are visible on the Exploring page.
- If enabled during the Folders installation, this variable must be manually disabled.

Figure A–3 Read-Only Icon

Figure A–4 Editable Icon

A.4.3.1 Manually Enabling CollectionReadOnlyMeta

To enable the Read-Only feature manually, complete the following steps:

1. Create a custom metadata field using Configuration Manager with the following parameters:
   - **Name =** ReadOnly
   - **Field Caption =** Read Only
   - **Field Type =** Text
   - **Enable on User Interface =** Selected
   - **Enable Option List =** Selected
   - **Option list values =** false and true

   Make sure that you update the database design in Configuration Manager to include the new field in your database. It is not necessary to rebuild your search index.
2. Add the following line to the Folders configuration file:

   ```
   CollectionReadOnlyMeta=xReadOnly
   ```

   You can name this field something other than ReadOnly, but the setting in the content server configuration file must match the field name. For example, if you name the field *Lock*, then `CollectionReadOnlyMeta=xLock`.

A.4.3.2 Manually Disabling CollectionReadOnlyMeta

To disable the Read-Only feature manually, complete the following steps:

1. In a text editor, open each of the following configuration files (this variable may be set in more than one file):
   - [*Instance_Dir*]/data/components/Folders/config.cfg (not for CS 6.2)
   - [*Instance_Dir*]/data/components/Folders/install.cfg
   - [*Instance_Dir*]/custom/Folders/folders_environment.cfg
   - [*Instance_Dir*]/config/config.cfg
2. Comment out the `CollectionReadOnlyMeta` configuration variable, if it exists, by preceding its line with a hash symbol (#).
3. Save and close the edited configuration files.

Make sure that you comment out the configuration variable. Simply editing the variable in the configuration files by deleting or changing the metadata field value will not reverse the functionality nor will it remove the Read-Only/Editable icons or Hidden metadata field from the user interface.

Commenting out the parameter line in the configuration file does not remove the ReadOnly metadata field from the database. If you want to clean up your database in regards to functionality that is not enabled, you may choose to remove the ReadOnly metadata field from the database. Please note that this requires the database design to be updated and the index rebuilt, which may take a considerable amount of time.

A.4.4 CollectionSecurityReadOnly

The **CollectionSecurityReadOnly** setting enables you to specify the user's folder and file security permissions that are evaluated when result sets are created. On certain layouts (for example, the Classic layout), this information is used to change the actions that are available to the user for the folders and content items.

- `CollectionSecurityReadOnly=true` specifies that only the Read security permission is evaluated.
- `CollectionSecurityReadOnly=false` specifies that all security permissions are evaluated (Read, Write, Delete, and Admin). Please note that this setting can slow down the content server considerably.
- Please note that regardless of the setting used, the user might see actions for which they do not have permission (depending the layout being used). However, the user will receive an error if they attempt to perform these actions.
- This variable is set to *true* by default, and it is recommended that you use this setting to avoid performance issues. Security permissions are evaluated according to this setting, even if the layout that is being used does not use this information to change the actions that are available to the user.

A.4.5 CollectionMoveEnabled

The **CollectionMoveEnabled** setting enables you to hide the move icon (see Figure A–5) or menu option on the Exploring pages.

- `CollectionMoveEnabled=true` displays the Move icon or option so that users can move folders and content items to other folders.
- `CollectionMoveEnabled=false` hides the Move icon or option so that users cannot move folders and content items to other folders.
- This variable is set automatically by the Folders installer program, according to the option you select.
- See also "CollectionMoveEnabled:actionPopup" on page A-15.

Figure A–5 Move Icon

A.4.6 CollectionDeleteEnabled

The **CollectionDeleteEnabled** setting enables you to hide the Delete icon (see Figure A–6) or menu option on the Exploring pages.

- `CollectionDeleteEnabled=true` displays the Delete icon or option so that users can delete folders and content items from an Exploring page.
- `CollectionDeleteEnabled=false` hides the Delete icon or option so that users cannot delete folders and content items from an Exploring page.
- This variable is set automatically by the Folders installer program, according to the option you select.

Figure A–6 Delete Icon

A.4.7 CollectionWebDAVServer

The **CollectionWebDAVServer** setting enables users to switch the view from a Content Server web page to a WebDAV folder in Windows Explorer.

```
CollectionWebDAVServer=webdav_URL
```

- For example, on a master content server, this setting would be:

  ```
  CollectionWebDAVServer=http://my_computer/web_root/idcplg/webdav
  ```

- You must install and configure WebDAV functionality on the content server to use this feature. See "About WebDAV" on page 1-1 for more information on WebDAV.
- In Microsoft Internet Explorer 5.0 or greater, this setting adds a WebDAV Icon to the virtual folder Exploring pages. The web folder icon is not displayed in any other browser.
- This variable is set automatically by the Folders installer program if you choose to install the WebDAV component.

Figure A–7 WebDAV Icon

A.4.8 CollectionInhibitUpdateMeta

The **CollectionInhibitUpdateMeta** setting defines an inhibit field for the metadata propagation function, which enables contributors to copy metadata values from a folder to its subfolders and content items.

- See the *Folders and WebDAV User Guide* and *Folders and WebDAV Administration Guide* for more information.
- This variable is set automatically by the Folders installer program, according to the field name you enter.

A.4.8.1 Enabling the Metadata Propagation Feature

To enable the Metadata Propagation feature, complete the following steps

1. Create a custom metadata field with the following parameters:
   - **Name =** CollectionInhibitUpdateMeta
   - **Field Caption =** Inhibit Metadata Update
   - **Field Type =** Text
   - **Enable on User Interface =** Selected
   - **Enable Option List =** Selected
   - **Option list values =** *false* and *true* (leaving the list blank is optional, and is interpreted as *false*).

   Make sure that you click **Update Database Design** to include the new field in your database. It is not necessary to rebuild your search index.
2. Add the following line to the configuration file:

   ```
   CollectionInhibitUpdateMeta=xCollectionInhibitUpdateMeta
   ```

You can name this field something other than CollectionInhibitUpdateMeta, but the setting in the content server configuration file must match the field name. For example, if you name the field *Inhibit*, then `CollectionInhibitUpdateMeta=xInhibit`.

A.4.9 CollectionForceFolderSecurityEnabled

The **CollectionForceFolderSecurityEnabled** setting specifies whether the Force Folder Security function is enabled.

- The Force Folder Security feature allows users to automatically propagate a containing folder's security attributes (Security Group and Document Account) onto any new, copied, or moved content placed into that folder. The containing folder's specific metadata field (by default, `xForceFolderSecurity`) can be set to TRUE or FALSE (or be empty, which is the same as FALSE). When the Force Folder Security feature is enabled, any folder that has its ForceFolderSecurity field set to FALSE will not trigger any new behavior, however, any folder that has its ForceFolderSecurity field set to TRUE will force any content entering the folder to have the content's security fields overridden to match the security fields of the folder.
- The default setting is `CollectionForceFolderSecurityEnabled=true`.
- If this setting is enabled during component installation, the feature can be disabled at a later time by setting CollectionForceFolderSecurityEnabled=false and restarting Content Server.
- See also "CollectionForceFolderSecurityMeta" on page A-9.

A.4.10 CollectionForceFolderSecurityMeta

The **CollectionForceFolderSecurityMeta** setting defines the metadata field name used to control the Force Folder Security status of individual folders.

- The Force Folder Security feature allows users to automatically propagate a containing folder's security attributes (Security Group and Document Account) onto any new, copied, or moved content placed into that folder. The containing folder's specific metadata field (by default, `xForceFolderSecurity`) can be set to TRUE or FALSE (or be empty, which is the same as FALSE). When the Force Folder Security feature is enabled, any folder that has its ForceFolderSecurity field set to FALSE will not trigger any new behavior, however, any folder that has its ForceFolderSecurity field set to TRUE will force any content entering the folder to have the content's security fields overridden to match the security fields of the folder.
- The default setting is `CollectionForceFolderSecurityMeta=xForceFolderSecurityMeta`.
- The value of this field has no meaning for individual content items.
- Generally, the only reason to change this value from its default setting would be if your Content Server already uses a metadata field of the same name.
- See also "CollectionForceFolderSecurityEnabled" on page A-9.

A.4.11 CollectionTrashDeleter

The **CollectionTrashDeleter** setting defines a user metadata field for the Trash function, which enables the user's login information to be recorded as metadata for items that are moved to the Trash folder.

- If this variable is set, users can choose whether to view only the items they have moved to the Trash folder or all of the items *everyone* has moved to the Trash folder. See the *Folders and WebDAV User Guide* for more information.
- This variable is set automatically by the Folders installer program if you choose to enable the Trash Bin function.

A.4.11.1 Enabling the Trash Deleter Feature

To enable the Trash Deleter feature manually, complete the following steps:

1. Create a custom metadata field with the following parameters:
   - **Name =** TrashDeleter
   - **Field Caption =** Trash Deleter
   - **Field Type =** Text
   - **Enable on User Interface =** Selected
   - **Enable Option List =** Clear

   Make sure that you click **Update Database Design** to include the new field in your database. It is not necessary to rebuild your search index.
2. Add the following line to the configuration file:

   ```
   CollectionTrashDeleter=xTrashDeleter
   ```

You can name this field something other than CollectionTrashDeleter, but the setting in the content server configuration file must match the field name. For example, if you name the field *TrashUser*, then `CollectionTrashDeleter=xTrashUser`.

A.4.12 CollectionTrashDeleteDate

The **CollectionTrashDeleteDate** setting defines a date metadata field for the Trash function, which enables the deletion date and time to be recorded as metadata for items that are moved to the Trash folder.

- If this variable is set, the deletion date and time are displayed in the Trash folder.
- This variable is set automatically by the Folders installer program if you choose to enable the Trash Bin function.

A.4.12.1 Enabling the Trash Delete Date Feature

To enable the Trash Delete Date feature manually, complete the following steps:

1. Create a custom metadata field with the following parameters:
   - **Name =** TrashDeleteDate
   - **Field Caption =** Trash Delete Date
   - **Field Type =** Date
   - **Enable on User Interface =** Selected
   - **Enable Option List =** Clear

Make sure that you click **Update Database Design** to include the new field in your database. It is not necessary to rebuild your search index.

2. Add the following line to the configuration file:

```
CollectionTrashDeleteDate=xTrashDeleteDate
```

You can name this field something other than CollectionTrashDeleteDate, but the setting in the content server configuration file must match the field name. For example, if you name the field *TrashDate*, then `CollectionTrashDeleteDate=xTrashDate`.

A.4.13 CollectionTrashDeleteLocation

The **CollectionTrashDeleteLocation** setting defines an integer metadata field for the Trash function, which enables the original parent folder to be recorded as metadata for items that are moved to the Trash folder.

- If this variable is set, users will be able to restore deleted items from the Trash folder. See Restoring Folders and Content from Trash (documented in the *Folders and WebDAV User Guide*).
- This variable is set automatically by the Folders installer program if you choose to enable the Trash Bin function.

A.4.13.1 Enabling the Trash Delete Location Feature

To enable the Trash Delete Location feature manually, complete the following steps:

1. Create a custom metadata field with the following parameters:
   - **Name =** TrashDeleteLocation
   - **Field Caption =** Trash Delete Location
   - **Field Type =** Integer
   - **Enable on User Interface =** Selected
   - **Enable Option List =** Clear

   Make sure that you click **Update Database Design** to include the new field in your database. It is not necessary to rebuild your search index.

2. Add the following line to the configuration file:

```
CollectionTrashDeleteLocation=xTrashDeleteLocation
```

You can name this field something other than CollectionTrashDeleteLocation, but the setting in the content server configuration file must match the field name. For example, if you name the field *TrashLoc*, then `CollectionTrashDeleteLocation=xTrashLoc`.

A.4.14 CollectionTrashDeleteOldName

The **CollectionTrashDeleteOldName** setting defines a file name metadata field for the Trash function, which enables the original file name to be recorded as metadata for items that are moved to the Trash folder.

- If this variable is set, files that are renamed due to a naming conflict in the Trash folder can be restored with their original file names. See Restoring Folders and Content from Trash (documented in the *Folders and WebDAV User Guide*).

- This variable is set automatically by the Folders installer program if you choose to enable the Trash Bin function.

A.4.14.1 Enabling the Trash Delete Old Name Feature

To enable the Trash Delete Old Name feature manually, complete the following steps:

1. Create a custom metadata field with the following parameters:
   - **Name =** TrashDeleteOldName
   - **Field Caption =** Trash Delete Old Name
   - **Field Type =** Memo
   - **Enable on User Interface =** Selected
   - **Enable Option List =** Clear

   Make sure that you click **Update Database Design** to include the new field in your database. It is not necessary to rebuild your search index.
2. Add the following line to the configuration file:

   ```
   CollectionTrashDeleteOldName=xTrashDeleteOldName
   ```

You can name this field something other than CollectionTrashDeleteOldName, but the setting in the content server configuration file must match the field name. For example, if you name the field *TrashName*, then `CollectionTrashDeleteOldName=xTrashName`.

A.4.15 FolderToTrashDeleteAccessIsStrict

The **FolderToTrashDeleteAccessIsStrict** setting prevents users from being able to delete Folders when any internal content of that folder (document items or other folders) cannot be deleted by that user.

By default, when a folder is deleted it is moved to the trash folder if the user has DELETE security rights on the folder, ignoring any internal content.

To enable this feature manually, complete the following steps:

1. In a text editor, open each of the following configuration files (this variable may be set in more than one file) and set `FolderToTrashDeleteAccessIsStrict=true`:
   - [*Instance_Dir*]/custom/Folders_g/folders_environment.cfg
   - [*Instance_Dir*]/data/components/folders_g/config.cfg
   - [*Instance_Dir*]/data/components/folders_g/install.cfg
2. Save and close the edited configuration files.
3. Restart Content Server.

A.4.16 CollectionReadOnlyMarkedFolders

The **CollectionReadOnlyMarkedFolders** setting enables you to specify whether the system-level folders can be modified.

- `CollectionReadOnlyMarkedFolders=true` prevents modification of the metadata for system-level folders such as Contribution Server Folders and Trash.

- `CollectionReadOnlyMarkedFolders=false` enables the ability to modify the metadata for system-level folders.
- This variable is set to *true* by default.

> **Caution:** If this variable is set to *false*, you should assign an appropriate security group to the system-level folders so that only authorized administrators can modify the folders. You should change system-level folders only if there is a particular reason to do so.

A.4.17 InitialColID

The **InitialColID** setting defines the counter that initializes the first collection ID.

- This is set during component installation. Use this to set the prefix where you want to start the counting of the folders.
- Defines the initial folder identifier for this server (in millions).
- The default is 0. It is recommended that if you use multiple content servers, each server should set a unique value. This will allow for online exchange of folders between content server instances.

A.4.18 CollectionReleasedOnly

The **CollectionReleasedOnly** setting determines which version of a revised document will be visible to the author and users with read access to the content item.

- `CollectionReleasedOnly=false` allows the author and all users with read access to the content item to see the latest version.
- `CollectionReleasedOnly=true` allows all users with read access to the content item to see the latest version when it is released.

  Regardless of the current state of the revised content item (whether the setting is true or false), the author always views the latest version of the document.
- This variable is set to *false* by default (i.e., the latest version of a revised content item is displayed to the author and all users with read access).
- If you want to change the value of this setting after Folders is installed, you must manually change it in the *[Instance_Dir]*/custom/folders/folders_environment.cfg file.

A.4.19 CollectionContentSecurity

The **CollectionContentSecurity** setting determines whether users can see secure content on Exploring pages if they have no access privileges to the secure content.

- If `CollectionContentSecurity=true`, then users with no access privileges to secure content will not see it on Exploring pages.
- If `CollectionContentSecurity=false`, then users with no access privileges to secure content will see it on Exploring pages. However, if they try to view the content, an "access-denied" error is displayed. This setting speeds up performance, but does allow users to see some information about secure content that they do not have access to.
- This variable is set to *true* by default.

A.4.20 CollectionFolderSecurity

The **CollectionFolderSecurity** setting determines whether users can see secure folders on Exploring pages if they have no access privileges to the secure folders.

- If `CollectionFolderSecurity=true`, then users with no access privileges to secure folders will not see them on Exploring pages.
- If `CollectionFolderSecurity=false`, then users with no access privileges to secure folders will see them on Exploring pages. However, if they try to open the folders, an "access-denied" error is displayed. This setting speeds up performance, but does allow users to see some information about secure content that they do not have access to.
- This variable is set to *true* by default.

A.4.21 CollectionUseCache

The CollectionUseCache setting determines whether items in folders are cached.

- If `CollectionUseCache=true`, then items in folders are cached.
- If `CollectionUseCache=false`, then items in folders are not cached.
- This variable is set to *true* by default.

Normally, there is no need to turn off this feature, but it may be useful in some situations (for example, for debugging purposes). To turn off caching, set the CollectionUseCache entry in the *[Instance_Dir]*/custom/folders/folders_environment.cfg file to 'false'. After modifying the folders_environment.cfg file, do not forget to restart the content server.

If folders caching is turned off (`CollectionUseCache=false`), content item shortcuts are not displayed.

If you reinstall or upgrade the Folders component, this configuration variable will revert back to its default setting (*true*). You can manually edit the folders_environment.cfg file again, or use a backed-up version.

A.4.22 CollectionDisplayResultSetSize

The **CollectionDisplayResultSetSize** setting specifies the maximum number of folders and content items that are displayed on Exploring pages. If the number of content 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.

> **Important:** If the number of folders exceeds value of `CollectionDisplayResultSetSize`, then the folders exceeding this value are not visible from Exploring pages. This means that if you already have more folders than this value or if your users add more folders than this value, those folders will not be visible from the Exploring pages.

- If this parameter is not set, the results are not truncated regardless of the number of items in the result set. This means that pages may be very long if there are many items to display.

- The parameter format is `CollectionDisplayResultSetSize=`*Number*, for example:

  ```
  CollectionDisplayResultSetSize=25
  ```

- The number of content items and folders are controlled by separate result sets, and are therefore treated separately. This means that if the parameter is set to 25, a maximum of 25 folders *and* 25 content items (for a total of 50 items) may be displayed on a single page.
- If a folder contains more subfolders than the CollectionDisplayResultSetSize value, then the main exploring page of that folder includes a Page Folders link. Clicking that link displays a new page, which lists the next series of subfolders contained in the parent folder. You can use the page navigation features to move between the list pages. However, each page will only show the subfolders in the parent folder and none of its content items. Similarly, if the number of content items in a folder exceeds the defined maximum, then that folder's main exploring page includes a Page Content link, which you can use to browse between the list pages. These pages will only show the content items in the parent folder, and no folders.

A.4.23 CollectionPropagateEmptyValues

The **CollectionPropagateEmptyValues** setting specifies whether empty field values are propagated.

- If `CollectionPropagateEmptyValues=true`, then empty field values are propagated.
- If `CollectionPropagateEmptyValues=false`, then empty field values are not propagated.
- The default is *true*.

To turn off propagation of empty field values, set the CollectionPropagateEmptyValues entry in the *[Instance_Dir]*/custom/folders/folders_environment.cfg file to 'false'. After modifying the folders_environment.cfg file, do not forget to restart the content server.

If you reinstall or upgrade the Folders component, this configuration variable will revert back to its default setting (true). You can manually edit the folders_environment.cfg file again, or use a backed-up version.

A.4.24 CollectionMoveEnabled:actionPopup

The **CollectionMoveEnabled:actionPopup** setting determines whether the Move option is included in the Actions popup menu for each item on an Exploring page.

- If `CollectionMoveEnabled:actionPopup=true`, then the Move option is included in the Actions popup menu.
- If `CollectionMoveEnabled:actionPopup=false`, then the Move option is not included in the Actions popup menu. This setting reduces the size of the page that is constructed and thus improves system performance.
- This configuration parameter does not disable the ability to move items altogether. It merely removes the option from the Actions popup menu for each item on Exploring pages.

- It is recommended that you put this configuration parameter in [*Instance_Dir*]/config/config.cfg rather than [*Instance_Dir*]/custom/folders/folders_environment.cfg. Otherwise it will be overwritten when Folders is upgraded.
- The Move menu option is only removed from the Actions popup menu next to the Info icons on Exploring pages, not from the Actions menu in the top right corner of the screen.
- See "CollectionMoveEnabled" on page A-7 if you want to disable the ability to move items altogether.

A.4.25 MaxHeadlineTableRows

If you have virtual folders with 1,000 items or more in them, then the first 999 rows will be displayed correctly on the exploring pages, but after that number some of the columns in the table are not visible. This can be avoided by adding the **MaxHeadlineTableRows** configuration variable in the [*Instance_Dir*]/custom/folders/folders_environment.cfg file and setting its value to a sufficiently high number, for example:

```
MaxHeadlineTableRows=1500
```

The table display issues will then become an issue only after the specified number of items is exceeded. After modifying the folders_environment.cfg file, do not forget to restart the content server.

Important: If you reinstall or upgrade the Folders component, you need to reapply this configuration variable or use a backed-up version of the folders_environment.cfg file.

A.4.26 CollectionSearchRecursiveContent

The **CollectionSearchRecursiveContent** setting enables a checkbox next to the Browse button of the search page for selecting a folder in the Folder metadata field. Selecting the checkbox will cause the search to include all content items in subfolders as well as in the selected folder.

- If `CollectionSearchRecursiveContent=true`, then the checkbox will appear on the search page.
- If `CollectionSearchRecursiveContent=false`, then the checkbox does not appear on the search page.
- The default setting is *false*.

A.4.27 CollectionMaxBranch

The **CollectionMaxBranch** setting determines the number of subfolder IDs that are collected by `CollectionSearchRecursiveContent` to be passed to the Search service when a Search is performed on a local folder. This setting can be used to tune performance by decreasing or increasing the number of subfolder IDs to be included in a Search.

- This setting is used when `CollectionSearchRecursiveContent=true`.
- The default setting is 100.

A.5 Configuration Variables for WebDAV

This section provides additional information about the following WebDAV configuration variables, which are defined in the *[Instance_Dir]*/custom/CoreWebDav/webdav_environment.cfg configuration file.

- CollectionWebDAVServer
- WebDAVReuseRevision
- WebDAVSecretKey
- WebDAVEnableFilterCookie
- WebDAVDisableOtherFilterCookies
- WebDAVEnableFilterUrlCookie
- WebDAVMaxInactiveInterval
- WebDAVDefaultTimeout
- WebDAVDoNotSetTitleToOriginalName

Even though you can set most WebDAV configuration parameters in [*Instance_Dir*]/config/config.cfg, it is strongly recommended that you set all WebDAV parameters in [*Instance_Dir*]/custom/CoreWebDav/webdav_environment.cfg, unless specifically stated otherwise. This allows disabling or uninstalling the WebDAV component to remove its entries automatically without forcing the administrator to look through other configuration and environment files on the server to delete the WebDAV-related entries manually.

Important: These configuration settings must be set in the WebDAV configuration file [*Instance_Dir*]/custom/CoreWebDav/webdav_environment.cfg. There is also an [*Instance_Dir*]/custom/folders/webdav_environment.cfg file, but this file is not used for normal WebDAV configuration purposes.

A.5.1 CollectionWebDAVServer

The **CollectionWebDAVServer** setting enables users to switch the view from a Folders and WebDAV web page to a WebDAV folder in Windows Explorer.

```
CollectionWebDAVServer=webdav_URL
```

- For example, on a master content server, this setting would be:

  ```
  CollectionWebDAVServer=http://my_computer/web_root/idcplg/webdav
  ```

- You must install and configure WebDAV functionality on the content server to use this feature. See "About WebDAV" on page 1-1 for more information on WebDAV.
- In Microsoft Internet Explorer 5.0 or greater, this setting adds a web folder icon to the virtual folder Exploring pages. The web folder icon is not displayed in any other browser.
- This variable is set automatically by the Folders installer program if you choose to install the WebDAV component.

A.5.2 WebDAVReuseRevision

The **WebDAVReuseRevision** setting specifies whether old revisions are deleted and new revisions created each time an open document is saved in a WebDAV folder. This setting is optional, but it is recommended to help prevent unnecessary revisions to a content item.

- For this setting to work correctly, the "Allow author to delete revision" setting in the content server must also be enabled (see ""Reuse Revision" Setting" on page 4-7).
- `WebDAVReuseRevision=false` means that each save (including auto-saves) will create a new revision.
- `WebDAVReuseRevision=true` means that not every save (including auto-saves) will create a new revision. This is useful to prevent a large number of unnecessary revisions.
- This variable is set to *true* by default.

A.5.3 WebDAVSecretKey

The **WebDAVSecretKey** setting is used to encrypt WebDAV login cookies on the local content server instance.

- This variable is set to *mysecret2003* by default.
- To prevent WebDAV login cookies from being used on other content servers, it is strongly recommended that you change this setting to a new, unique value for each content server instance that is accessed through WebDAV (see "Setting the WebDAV Secret Key" on page 4-7).

A.5.4 WebDAVEnableFilterCookie

The **WebDAVEnableFilterCookie** setting enables or disables persistent WebDAV login cookies in the web server filter. These cookies allow WebDAV compliant applications such as Word to open documents without prompting for a login.

- `WebDAVEnableFilterCookie=true` enables persistent WebDAV login cookies in the web server filter.
- `WebDAVEnableFilterCookie=false` disables persistent WebDAV login cookies in the web server filter.
- This variable is set to *true* by default.

A.5.5 WebDAVDisableOtherFilterCookies

The **WebDAVDisableOtherFilterCookies** setting enables or disables forms-based logins. The WebDAV component uses CookieLoginPlugin.dll for cookie-based login. The cookies eliminate additional login prompts when Microsoft Word opens a document using WebDAV. By default, the component keeps the dll file from doing forms-based logins on web pages by preventing redirects to a page with a login form instead of responding with an HTTP 401 status code which causes the browser to display a login prompt.

- `WebDAVDisableOtherFilterCookies=true` prevents redirects to web pages with a login form and displays a login prompt instead.

- `WebDAVDisableOtherFilterCookies=false` uses redirects instead of sending the HTTP 401 status code.
- This variable is set to *true* by default.

A.5.6 WebDAVEnableFilterUrlCookie

The **WebDAVEnableFilterUrlCookie** setting enables or disables login cookies being passed on as a URL parameter, which allows a WebDAV client interface to bypass the login prompt.

- `WebDAVEnableFilterUrlCookie=true` means that login cookies can be passed on as a URL parameter, which allows a WebDAV client interface to bypass the login prompt.
- `WebDAVEnableFilterUrlCookie=false` means that login cookies cannot be passed on as a URL parameter.
- This variable is set to *true* by default.

A.5.7 WebDAVMaxInactiveInterval

The **WebDAVMaxInactiveInterval** setting specifies the time (in seconds) between client requests before the client cookie expires.

- This variable is set to 7200 (or two hours) by default.
- This variable should be specified in the WebDAV configuration file [*Instance_Dir*]/custom/webdav/webdav_environment.cfg. There may already be an instance of this variable in [*Instance_Dir*]/custom/folders/webdav_environment.cfg (generally set to 3600), but this instance is ignored for normal WebDAV operation.
- If you remove the `WebDAVMaxInactiveInterval` entry from the [*Instance_Dir*]/custom/webdav/webdav_environment.cfg file or specify an unparsable entry, the variable defaults to 3600 (one hour).

A.5.8 WebDAVDefaultTimeout

The **WebDAVDefaultTimeout** setting specifies the time (in seconds) that a file opened through WebDAV remains locked (checked out) if the WebDAV client does not specify a timeout value. After this time, an "Undo Checkout" operation is performed on checked-out content.

- This variable is set to *Second-60* by default.
- The unit identifier "Second-" must be included.

A.5.9 WebDAVDoNotSetTitleToOriginalName

The **WebDAVDoNotSetTitleToOriginalName** setting controls how the title allocation of new content checked into the content server through WebDAV is handled.

- `WebDAVDoNotSetTitleToOriginalName=true` means that the title of a checked-in content item is allocated as follows:
  - If a default title metadata value has been defined for the folder that the content item is dropped into, then the title of the checked-in file will be the default title defined for the folder (for example, "Monthly Report").

  - If no default title metadata value has been defined for the folder, then the title of the checked-in file will always be the file name including the file extension (for example, "monthly_report_0412.doc").

- `WebDAVDoNotSetTitleToOriginalName=false` means that the title of a checked-in file will always be the file name without the file extension, regardless of whether a default title metadata value for the folder has been defined (for example, "monthly_report_0412").
- This variable is set to *false* by default.

For details on default metadata values for folders see the *Folders and WebDAV User Guide*.

B

Installation Details

This section explains the actions that are performed automatically during installation of the Folders component. The information is intended to help system administrators verify the installation and configuration, and to assist in troubleshooting.

This section covers the following topics:

B.1 Installation of Components

The installer unpackages and enables the components contained in the main Folders_g.zip component installation file, according to the selections made during the installation process. The Folders_g.zip component zip file contains the following sub-components:

- **Folders**: This is the main component that provides the folders functionality.
- **Helper**: This component contains generic content server functionality that is reused in many places. This component also is required by Universal Records Management (URM).

In some cases, manual configuration of the web server is required for WebDAV support. See Chapter 4, "Post-Installation Tasks and Considerations".

B.2 CollectionID Metadata Field

The installer performs the following tasks to add the Collection ID metadata field, which is used to store the unique Collection ID for each virtual folder:

1. It adds the metadata field to Configuration Manager with the following parameters:

Property	Value
Name	Entered during installation (default is *CollectionID*)
Field Caption	Folder

Property	Value
Field Type	Integer
Require Value	No
Enable for User Interface	Yes
Enable for Search Index	Yes
Enable Option List	No

2. It places an index on the field in the DocMeta database table.
3. It sets the value of the CollectionMeta entry in the Folders component configuration file ([*Instance_Dir*]/custom/folders_g/folders_environment.cfg) to the name of the new metadata field. For example:

```
CollectionMeta=xColID
```

B.3 Inhibit Metadata Update Field

The installer performs the following tasks to add the Inhibit metadata field, which is used to inhibit or allow metadata propagation:

1. It adds the metadata field to Configuration Manager with the following parameters:

Property	Value
Name	CollectionInhibitUpdateMeta
Field Caption	Inhibit Metadata Update
Field Type	Text
Require Value	No
Enable for User Interface	Yes
Enable for Search Index	Yes
Enable Option List	Yes; options are *false* (default) and *true*

2. It sets the value of the CollectionInhibitUpdateMeta entry in the Folders component configuration file ([*Instance_Dir*]/custom/folders_g/folders_environment.cfg) to the name of the new metadata field. For example:

```
CollectionInhibitUpdateMeta=xCollectionInhibitUpdateMeta
```

B.4 Folders/WebDAV Configuration Settings

The installer sets the following entries in the Folders component configuration file [*Instance_Dir*]/custom/folders_g/folders_environment.cfg) according to user selections:

Entry	Description
CollectionHiddenMeta=xHidden	Defines whether users can specify if a virtual folder or content item is hidden or visible. ■ If enabled during installation, the field name must also be specified during installation. ■ See "CollectionHiddenMeta" on page A-4 for further details.
CollectionReadOnlyMeta=xReadOnly	Defines whether users can specify if a virtual folder and its contents are read-only. ■ If enabled during installation, the field name must also be specified during installation. ■ See "CollectionReadOnlyMeta" on page A-5 for further details.
CollectionMoveEnabled=true	■ Defines whether the Move icon is displayed so that users can move folders and content items to other folders. ■ Specified during installation. ■ See "CollectionMoveEnabled" on page A-7 for further details.
CollectionDeleteEnabled=true	Defines whether the Delete icon is displayed so that users can delete folders and content items. ■ Specified during installation. ■ See "CollectionDeleteEnabled" on page A-7 for further details.
CollectionWebDAVServer= http://*<server>*/*<webroot>*/idcplg/webdav	Defines whether users can switch the view from a virtual folder on a content server web page to a WebDAV folder. ■ If the WebDAV component is installed, this setting is defined. ■ See "CollectionWebDAVServer" on page A-17 for further details.
CollectionTrashDeleter=xTrashDeleter	Defines a metadata field for recording the user who deleted an item as metadata. ■ Specified during installation (all Trash Bin settings are enabled or disabled). ■ See "CollectionTrashDeleter" on page A-10 for further details.
CollectionTrashDeleteDate= xTrashDeleteDate	Defines a metadata field for recording the deletion date and time as metadata. ■ Specified during installation (all Trash Bin settings are enabled or disabled). ■ See "CollectionTrashDeleteDate" on page A-10 for further details.
CollectionTrashDeleteLocation= xTrashDeleteLocation	Defines a metadata field for recording the parent folder of a deleted item as metadata. ■ Specified during installation (all Trash Bin settings are enabled or disabled). ■ See "CollectionTrashDeleteLocation" on page A-11 for further details.

Entry	Description
CollectionTrashDeleteOldName=xTrashDeleteOldName	Defines whether to record the original name of deleted items as metadata. ■ Specified during installation (all Trash Bin settings are enabled or disabled). ■ See "CollectionTrashDeleteOldName" on page A-11 for further details.
CollectionReadOnlyMarkedFolders=true	Defines whether system-level folders can be modified. ■ Set to *true* by default. ■ See "CollectionReadOnlyMarkedFolders" on page A-12 for further details.
ForceFolderSecurity=true	Enables a Folder to be configured to that any new, copied, or moved content item or folder placed into the Folder will automatically be set to the containing Folder's security attributes. ■ Set to *true* by default. ■ See "CollectionForceFolderSecurityEnabled" on page A-9 for further details.
InitialColID=0	Defines the counter that initializes the first collection ID. ■ Specified during installation. ■ See "InitialColID" on page A-13 for further details.
CollectionReleasedOnly=false	Determines the visibility of a revised document to the author and users with read access to the content item. ■ Set to *false* by default. ■ See "CollectionReleasedOnly" on page A-13 for further details.

B.5 Folder and File Limits

The installer sets up the folder and file limits in accordance with the values you entered during installation. These values can be changed on the Virtual Folder Administration Configuration page in the content server. See the *Folders and WebDAV Administration Guide* for more information.

Important: Setting the folder and file limits too high may affect system performance, and also makes it harder for users to browse through folders. It is recommended that you do not exceed 1,000 folders and 1,000 content items in a virtual folder.

B.6 Folders and WebDAV Configuration Settings

The installer sets the following content server system properties in the content server configuration file ([*Instance_Dir*]/config/config.cfg):

Setting	Description
GetCopyAccess=true	Enables the "Allow get copy for user with read privilege" setting, which allows users to get a copy of a content item for which they have only Read permission.
AuthorDelete=true	If WebDAV is enabled, the "Allow author to delete revision" setting is set to *true*. This allows the last revision to be deleted when a file is saved so that unnecessary revisions are not created. See ""Reuse Revision" Setting" on page 4-7.

C

Uninstalling Folders

This section covers the following topics:

An automated uninstallation using Component Manager is sufficient for most users. However, if you want to completely remove the Folders component from the content server, you must uninstall it manually. An automated uninstallation only removes the component, not the database tables, metadata fields, and directories.

C.1 Automated Uninstallation

The Folders component cannot be uninstalled using Component Wizard. Use Component Manager to disable or uninstall the Folders component:

1. Open a new browser window and log into the content server as a system administrator.
2. Go to the Administration Applets page and click the **Admin Server** link.
3. On the Content Admin Server page, click the button of the content server instance that you want to uninstall the Folders component from.

   The status page for the content server instance is displayed.
4. In the option list for the server instance, click the **Component Manager** link.

   The Component Manager page is displayed.
5. Disable the Folders (or Folders_g) component that you want to uninstall:
   a. Select each component in the Enabled Components list.
   b. Click the **Disable** button to move it to the Disabled Components list.

   The following components may be installed with Folders (depending on the options selected during installation):

   - Folders (or Folders_g)
   - Helper
6. Click **Start/Stop Content Server** in the left navigation menu.
7. Click the Restart icon to restart the content server.
8. Click **Component Manager** in the left navigation menu to return to the Component Manager page.

9. Select the Folders (or Folders_g) component in the **Uninstall Component** list, and click **Uninstall**.
10. A prompt is displayed asking you to confirm the uninstallation process of the selected component. Click **OK** to confirm. The Folders-related components in the Disabled Components list are automatically uninstalled along with the Folders component.
11. After uninstalling all components, restart the content server.

Important: The Microsoft SQL Server Data Engine (MSDE) does not support drop index commands. Therefore, if you are using MSDE as the database, you may receive an error message during the uninstall process (such as "Could not drop index for column xCollectionID of table DocMeta"). If this occurs, continue with the uninstall procedure and have your database administrator remove the index manually.

C.2 Manual Uninstallation

The Folders uninstaller will remove the Folders component, but it will still leave some database tables and fields along with some directories on the file system. If you want to remove all remnants of Folders after uninstalling the component, you need to remove these other objects manually.

The procedure here deletes all existing Folders metadata fields and collection IDs. If you prefer, you can keep these existing metadata fields and collection IDs without harm. The documents already checked in will still have collection IDs linking them to a folder along with other Folders metadata, but these folders will no longer exist. If you reinstall Folders later, the collection IDs will start at the next collection ID in the Counters table. To keep the existing Folders metadata fields and collection IDs, you need to only perform steps 1, 2, and 5 below. The other steps can then be skipped. To reset the collection ID, make sure that you perform all steps.

1. Drop the following database tables in this order (if they still exist):
   a. Links
   b. ColMeta
   c. Collections
2. Delete any Folders-specific rows from the Config database table. These are all rows in this table where the value of dName is equal to "Folders" or "folders_g".
3. Delete the ColID row from the Counters database table.
4. Delete the xCollectionID index from the DocMeta table.
5. Delete the following directories (if they still exist):
   a. [*Instance_Dir*]/custom/folders_g
   b. [*Instance_Dir*]/classes/collections
   c. [*Instance_Dir*]/data/components/folders_g
   d. [*Instance_Dir*]/data/events
   e. [*Instance_Dir*]/data/collectionconfig
6. Delete the collectionuserconfig.hda file from [*Instance_Dir*]/data/users/profiles/sy/sysadmin. This step removes the folder settings for sysadmin. If you want to remove the folder settings of other users as well, you must delete the

collectionuserconfig.hda file under [*Instance_Dir*]/data/users/profiles for each individual user.

7. Use Configuration Manager to delete the following information fields (if they exist):
   a. CollectionID
   b. Hidden
   c. InhibitUpdate
   d. ReadOnly
   e. TrashDeleteDate
   f. TrashDeleteLoc
   g. TrashDeleteName
   h. TrashDeleter

   The names of the fields in your instance may be different from the default names listed here depending on what names you chose when you installed Folders.
8. After deleting the listed fields, click the **Update Database Design** button in Configuration Manager. Verify that the above fields are all listed in the next window and then click **OK**.
9. If the **Rebuild Search Index** button is enabled, it is recommended that you click the button to remove all the deleted fields from the search index.

D

Third Party Licenses

This appendix includes a description of the Third Party Licenses for all the third party products included with this product.

D.1 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.
```

D.2 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.
*
```

D.3 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

D.4 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.

D.5 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.

D.6 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

D.7 Miscellaneous Attributions

Adobe, Acrobat, and the Acrobat Logo are registered trademarks of Adobe Systems Incorporated.
FAST Instream is a trademark of Fast Search and Transfer ASA.
HP-UX is a registered trademark of Hewlett-Packard Company.
IBM, Informix, and DB2 are registered trademarks of IBM Corporation.
Jaws PDF Library is a registered trademark of Global Graphics Software Ltd.
Kofax is a registered trademark, and Ascent and Ascent Capture are trademarks of Kofax Image Products.
Linux is a registered trademark of Linus Torvalds.
Mac is a registered trademark, and Safari is a trademark of Apple Computer, Inc.
Microsoft, Windows, and Internet Explorer are registered trademarks of Microsoft Corporation.
MrSID is property of LizardTech, Inc. It is protected by U.S. Patent No. 5,710,835. Foreign Patents Pending.
Oracle is a registered trademark of Oracle Corporation.
Portions Copyright 1994-1997 LEAD Technologies, Inc. All rights reserved.
Portions Copyright 1990-1998 Handmade Software, Inc. All rights reserved.
Portions Copyright 1988, 1997 Aladdin Enterprises. All rights reserved.
Portions Copyright 1997 Soft Horizons. All rights reserved.
Portions Copyright 1995-1999 LizardTech, Inc. All rights reserved.
Red Hat is a registered trademark of Red Hat, Inc.
Sun is a registered trademark, and Sun ONE, Solaris, iPlanet and Java are trademarks of Sun Microsystems, Inc.
Sybase is a registered trademark of Sybase, Inc.

UNIX is a registered trademark of The Open Group.
Verity is a registered trademark of Autonomy Corporation plc

Index

A

B

C

D

E

F

G

H

I

K

L

M

P

R

S

T

U

V

W