Desktop Integration Suite Installation Guide
10*g* Release 3 (10.1.3.3.1)

July 2007

ORACLE

Desktop Integration Suite Installation Guide, 10*g* Release 3 (10.1.3.3.1)

Contributing author: Ron van de Crommert

Chapter 5: Configuring Windows Explorer

Chapter 6: Integrating Adobe Acrobat Capture

Chapter 7: Content Server Administration Notes

1

INTRODUCTION

ABOUT DESKTOP INTEGRATION SUITE

Desktop Integration Suite (DIS) allows you to integrate Content Server functionality with a number of desktop applications. These integrations enable users to manage content on the content server directly from their workstations, as well as share documents with other users throughout the organization.

Desktop Integration Suite provides the following integration options:

❖ **Windows Explorer integration—**This integration enables you to access the content server and create folders in Windows Explorer.

❖ **E-mail client integration**—This integration enables you to check e-mail messages and attachments into and out of the content server, directly from your e-mail client. Using Microsoft Outlook or Lotus Notes, you can navigate folders, drag and drop e-mail messages and attachments, and more between the e-mail client and the content server.

❖ **Desktop application integration**—This integration allows you to check documents into and out of the content server directly from a number of supported desktop applications, rather than through web browser interface of the content server. See page 2-1 for a list of available desktop applications.

ABOUT THIS GUIDE

This document provides the information that you need to install the Desktop Integration Suite software and set up the content server and client workstations to access the integration features.

AVAILABLE DOCUMENTATION

The following documentation is available in your Desktop installation folder and in the software distribution package:

❖ **Desktop Integration Suite Installation Guide** (this document)—Provides instructions for installing and setting up the Desktop Integration Suite software. It is available as a PDF file.

❖ **Desktop Integration Suite User Guide**—Explains how to work with files and folders in the content server using Windows Explorer, your e-mail client (Microsoft Outlook or Lotus Notes Email), and your desktop application (Microsoft Word, Excel, PowerPoint, etc.). It is available as an online Help system and PDF.

Viewing the User Guide From the Software

The Desktop Integration Suite User Guide can be opened from various places in each application.

❖ In Windows Explorer, select a Content Server Folder (or content within it) and then click **Help—Help Topics**.

❖ In Microsoft Outlook, click **Help—Email Client Integration Help**.

❖ In Lotus Notes Email, click **Actions—Email Client Integration Help**.

❖ In all other applications (including Windows Explorer and your e-mail client), click the **Help** button (Help) or the **Help** icon (?) that appears in the Desktop-generated dialog boxes.

Viewing Help Files in Internet Explorer

The Help systems in Desktop Integration Suite use client-side JavaScript to display the Contents pane. If you are running Windows XP Service Pack 2 and open Help from one of the applications, you may not see its contents because Internet Explorer, by default, prevents users from viewing active content on a local file system.

To view the Help system, click the information bar and choose **Allow Blocked Content**.

Figure 1-1   Information bar
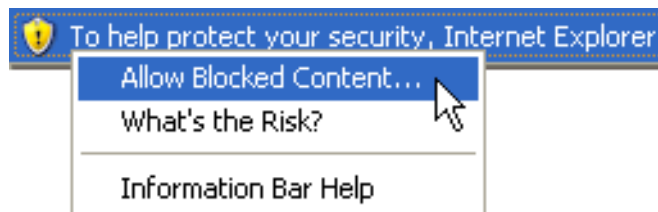
To avoid seeing this message again, go to Tool > Options > Advanced tab, and make sure the "Allow active content to run in files on My Computer" check box is selected.

2

REQUIREMENTS

OVERVIEW

This section covers the following topcis:

❖ Applications Supported (page 2-1)

❖ System Requirements (page 2-2)

❖ Installation Process (page 2-3)

APPLICATIONS SUPPORTED

Desktop Client Integration can integrate each of the following applications with Content Server. The installer automatically detects the supported applications and installs the appropriate integration features to provide those applications direct access to content server functionality. After you have installed these integrations, you will need to configure the content servers you want to work with.

Windows Explorer

❖ Microsoft Windows 2000 (SP1 or later)

❖ Microsoft Windows XP

❖ Microsoft Windows Vista

Desktop Applications

❖ Microsoft Word 2000 or higher

❖ Microsoft PowerPoint 2000 (SR-1) or higher

❖ Microsoft Excel 2000 or higher

❖ Microsoft Visio 2000 or higher

❖ Corel WordPerfect 10 or higher

❖ Lotus WordPro 9 or higher

❖ Adobe Acrobat Capture 3.0

E-Mail Clients

❖ Microsoft Outlook 2000 or higher

❖ Lotus Notes Email Client 6.5.2 or higher

SYSTEM REQUIREMENTS

To successfully integrate Content Server functionality with one of the supported applications (see page 2-1), you need:

❖ Content Server version 6.2, 7.1.1, 7.5 (including 7.5.*x*), or 10*g*R3 on the server

❖ the CoreWebDAV component (on Content Server 10*g*R3, see page 3-3)

❖ Microsoft Windows 2000 (SP1 or later), Windows XP, or Windows Vista with Microsoft Internet Explorer 6.0 or higher on each client. (Internet Explorer does not need to be the default browser.)

If you are integrating Content Server functionality with Windows Explorer, there are additional configuration considerations. See Chapter 5 (*Configuring Windows Explorer)*.

INSTALLATION PROCESS

To successfully use Desktop Integration Suite, you need to complete the following steps for the content server(s) and the client computers.

Content Server

❖ Uninstall any previous components, if required (see page 3-1)

❖ Install the latest components (see page 3-3)

❖ Configure the server after the new components are installed (see page 3-5)

Client Computers

❖ Uninstall any previous versions of the Desktop Integration Suite client software (see page 4-2)

❖ Install the latest Desktop Integration Suite software (see page 4-2)

❖ Configure the client computers for server connections (see page 4-5)

❖ Configure the client computers for metadata options (see page 4-5)

3

SETTING UP
THE CONTENT SERVER

OVERVIEW

The installation and setup of Desktop Integration Suite is a multi-step process for both the content server and the client computers to be used with the content server. This chapter discusses the processes to set up Desktop Integration Suite on the content server. See Chapter 4 (*Setting Up the Client Computers)* for details about installation on client computers.

This section covers the following topics:

❖ Uninstalling Previous Components (page 3-1)

❖ Installing New Components (page 3-3)

❖ Adding E-Mail Metadata Fields Manually (page 3-5)

❖ Configuring Netegrity SiteMinder (page 3-7)

UNINSTALLING PREVIOUS COMPONENTS

This section covers the following topics:

❖ Components To Be Uninstalled (page 3-2)

❖ Uninstalling Components (page 3-2)

Components To Be Uninstalled

If any of the following components are installed on the content server, you need to uninstall them:

❖ **WebdavClientHelper**—If you are using Content Server 7.*x*, you must disable the WebdavClientHelper70 component. The Desktop Integration Suite component has this functionality built in.

Note: If you are using Content Server 6.2, you must update the existing WebdavClientHelper65 component with the one provided in the Desktop Integration Suite distribution package.

❖ **OutlookIntegration**—Uninstall this component.

❖ **ODMA7**—Uninstall this component.

Uninstalling Components

To uninstall a component on the content server, complete the following steps:

1. Open a new browser window and log into 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 component(s) 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 all components that you want to uninstall (see above):

   a. Select each component in the Enabled Components list.

   b. Click the **Disable** button to move it to the Disabled Components list.

6. Restart the content server.

7. Go back to the Component Manager page.

8. Select a disabled component to be uninstalled in the Uninstall Component dropdown list, and click **Uninstall**.

9. A prompt is displayed asking you to confirm the uninstallation process of the selected component. Click **OK** to confirm.

10. After the component has been uninstalled, a message is displayed stating that the component was uninstalled successfully.

    Click on the link to return to Component Manager.

11. Repeat steps 8 through 10 for each disabled component to be uninstalled.

12. After uninstalling all components, restart the content server.

Note: Uninstalling a component means that the content server no longer recognizes the component, but the component files are not deleted from the file system.

INSTALLING NEW COMPONENTS

This section covers the following topics:

❖ Required Components (page 3-3)

❖ Installing Components (page 3-4)

Required Components

You need to have the following components installed and enabled on the content server(s) that you plan to use with Desktop Integration Suite:

❖ **DesktopIntegrationSuite**—This component provides core desktop integration functionality and is a required component. It is included in the Desktop Integration Suite distribution package (in the *Component* directory).

❖ **CoreWebDav** (for Content Server 10*g*R3)—This component provides core WebDAV functionality and is a required component for Desktop Integration Suite to work with Content Server 10*g*R3. You can install the CoreWebDAV component as part of the Content Server 10*g*R3 installation process. (It is included in the list of optional components, and it is selected for installation by default.) If you need to install this component after installing the Content Server software, then you can find it in the *\packages\allplatform* directory of the Content Server 10*g*R3 distribution package.

❖ **WebDav** (for earlier Content Server releases)—This component is required for Content Server releases prior to 10*g*R3 to provide Windows Explorer integration and Content Server folders in your e-mail client (Microsoft Outlook or Lotus Notes).

❖ **Folders**—This component is required for Windows Explorer integration (see chapter 5) and for the Content Server folders features in your e-mail client (Microsoft Outlook or Lotus Notes). You can find this component in the *extras* directory of the Content Server 10*g*R3 distribution package. Make sure that you choose to install the Folders WebDAV component in the installation options (this is not the default).

❖ **WebdavClientHelper**—If you are using Content Server 6.2, you must update the WebdavClientHelper65 component with the one provided in the Desktop Integration Suite distribution package (in the *Component* directory).

❖ **EmailMetadata**—This component is recommended if you will be using the Content Server folders features in Microsoft Outlook or Lotus Notes. It is included in the Desktop Integration Suite distribution package (in the *Component* directory).

❖ **RmaEmail**— This component is optional for Microsoft Outlook or Lotus Notes integration. It enables you to check in e-mail distribution lists. It is part of the Universal Records Management (URM) software.

If you are planning to use multiple content servers to manage content from your desktop, it is recommended that you set up each content server in exactly the same.

Installing Components

When you install a component, you may have more than one version to choose from. Be sure to choose the component that matches the version of the content server you are running.

Determining the Content Server Version

To determine the version of the content server you are running, perform the following steps on the content server:

1. Open a new browser window and log into Content Server as a system administrator.

2. In the Administration menu, click **Admin Server.**

3. Click **View Admin Output**.

    The server version is shown at the top of the console output, for example:
    ```
    Admin Server Version 10.1.3.3.1 (070511)
    ```

Installing and Enabling a Component

To install a component on the content server, complete the following steps:

1. Open a new browser window and log into Content Server as a system administrator (with the "sysmanager" role).

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 install the component(s) on.

   The status page for the selected 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. Click the **Browse** button next to the **Install New Component** field.

6. Navigate to the component zip file to be installed (see page 3-3), select it, and close the file selection dialog.

7. Click **Install**. An overview page is displayed providing a list of the items that will be installed.

8. Click **Continue**. All required files are now uploaded and installed.

Note: The upload may take a long time, especially when installing onto a network drive, and there is no indication of progress. Perform the upload on a browser running on the same machine as the content server.

9. Repeat this process for each component to be installed.

   After all files have been copied, a message is displayed stating that the components were uploaded and installed successfully.

ADDING E-MAIL METADATA FIELDS MANUALLY

If you do not install the RmaEmail component, you can still add e-mail specific metadata fields to the content server to capture key information at check-in. If used, these metadata fields are pre-populated with available values when you check an e-mail or attachment into the server. The metadata are optional and are not required to integrate Content Server with your e-mail client.

Field name	Field type	Enable on user interface	Enable for search index	Suggested field caption
EmailFrom	Text	Yes	Yes	Author or Originator
EmailTo	Memo	Yes	Yes	Addressee(s)
EmailCC	Memo	Yes	Yes	Other Addressee(s)
EmailSubject	Long Text	Yes	Yes	Email Subject
PublicationDate	Date	Yes	Yes	Publication Date
ReceivedDate	Date	Yes	Yes	Received Date

Caution: If you manually add the e-mail specific metadata fields listed above, you may need to rebuild your search index (for example, if you are not using database searching and indexing). This may be a very time-consuming process, depending on the number of content items managed by your Content Server instance. It is therefore recommended that you perform this rebuild during off-peak hours of Content Server use (typically at night or on the weekend).

To manually add e-mail specific metadata fields, complete the following steps:

1. Open Content Server's Configuration Manager utility.

2. Select the **Information Fields** tab and click **Add**.

   The Add Metadata Field Name dialog is displayed.

3. Enter the metadata field name in accordance with the table above (for example, **EmailFrom**), and click **OK**.

   The Add Metadata Field dialog is displayed.

4. Configure the properties for the field, and ensure that the field type matches the type listed in the table above. Click **OK** when you are done. When you add the field caption (i.e., what is displayed in the content server interface), you can use any name you wish. (See suggested field captions in the table above.)

5. Repeat steps 2 to 4 for each e-mail specific metadata field you are adding to the content server.

6. Click **Update Database Design**.

7. Verify the new field names on the Update Database Design dialog and click **OK**.

8. Close the Configuration Manager utility.

CONFIGURING NETEGRITY SITEMINDER

Netegrity SiteMinder is an enterprise-scale authentication and authorization management application that runs on your network. Desktop is compatible with SiteMinder, and the two applications can be used together so that Desktop users can log onto the site using Netegrity's secure, form-based login screen.

Figure 3-1   Netegrity login

To set this up, you will need to add a comment to the SiteMinder login page so that Desktop identifies an HTML response as the forms-based login page. Users, as a result, will see the SiteMinder login instead of the standard content server login.

1. Browse the file system for the SiteMinder login form (example: `login.fcc`).

   The location of this form depends on how you set up Netegrity SiteMinder at your organization.

2. Open the form in a text editor.

3. Add the following comment (with no spaces) to the HEAD of the form:

   ```
   <!--IdcClientLoginForm=1-->
   ```

4. Save and close the form.

   For more information on customizing this form, see the SiteMinder documentation that accompanies the product.

The next time users log onto the content server in Desktop, they will see the Netegrity SiteMinder login form.

4

SETTING UP THE CLIENT COMPUTERS

OVERVIEW

The installation and setup of Desktop Integration Suite is a multi-step process for both the content server and the client computers to be used with the content server. This chapter discusses the processes to set up Desktop Integration Suite on the client computers. See Chapter 3 (*Setting Up the Content Server)* for details about installation on the content server.

This section covers the following topics:

- ❖ Installation Process (page 4-2)

- ❖ Uninstalling a Previous Version of Desktop Integration Suite (page 4-2)

- ❖ Installing the Latest Version of Desktop Integration Suite (page 4-2)

- ❖ Manually Configuring the Notes.ini File (page 4-4)

- ❖ Configuring Server Connections and Metadata (page 4-5)

- ❖ Uninstalling Desktop Integration Suite (page 4-13)

INSTALLATION PROCESS

To successfully run Desktop Client Integration, you need to perform the following steps on each client computer:

1. Uninstall any previous version of Desktop Integration Suite (see page 4-2)

2. Install the latest version of Desktop Integration Suite (see page 4-2)

3. Configure server connections and metadata (see page 4-5)

INSTALLATION CONSIDERATIONS

Please note the following considerations with regard to setting up a client computer for use with Desktop Integration Suite:

❖ The Desktop Integration Suite software must be installed using Administrator-level permissions. If a user without these permissions tries to install the software, the registry settings will not be properly set up.

❖ The client software of Desktop Integration Suite 10*g*R3 can communicate with Content Server versions 6.2, 7.1.1, 7.5 (including 7.5.*x*), and 10*g*R3.

UNINSTALLING A PREVIOUS VERSION OF DESKTOP INTEGRATION SUITE

You need to run the Desktop uninstaller to uninstall previous versions of Desktop. It is important that you completely uninstall everything previously installed. For additional information, see Uninstalling Desktop Integration Suite (page 4-13).

If you are running the WebDAV Client, you must uninstall it using the WebDAV Client uninstaller.

INSTALLING THE LATEST VERSION OF DESKTOP INTEGRATION SUITE

If there are no previous versions of Desktop Integration Suite or WebDAV Client on the client computer, you can install the current version of the Desktop Integration Suite client software.

Note: See Appendix A (*Custom Installation Options*) for information on silent, unattended installation options.

Follow these steps to install the Desktop Integration Suite client software:

1. Browse to the folder that contains the unzipped software distribution package for Desktop Integration Suite.

2. Double-click **setup.exe** in the root directory.

Note: Do not double-click **DesktopIntegrationSuite.msi** in the same location. This file can be used by administrators for specific client installation needs. See Appendix A (*Custom Installation Options*) for further details.

3. On the Welcome screen, click **Next** to start the installation.

4. On the Custom Setup screen, select the supported application(s) you want to integrate with Content Server.

    The list includes all supported applications on the local computer. All applications are selected for integration by default. If you do not want to integrate an application with Content Server, click its icon and choose "This feature will not be available." The icon associated with the application then changes to a red 'X'.

Figure 4-1   Selection of applications to integrate with Content Server
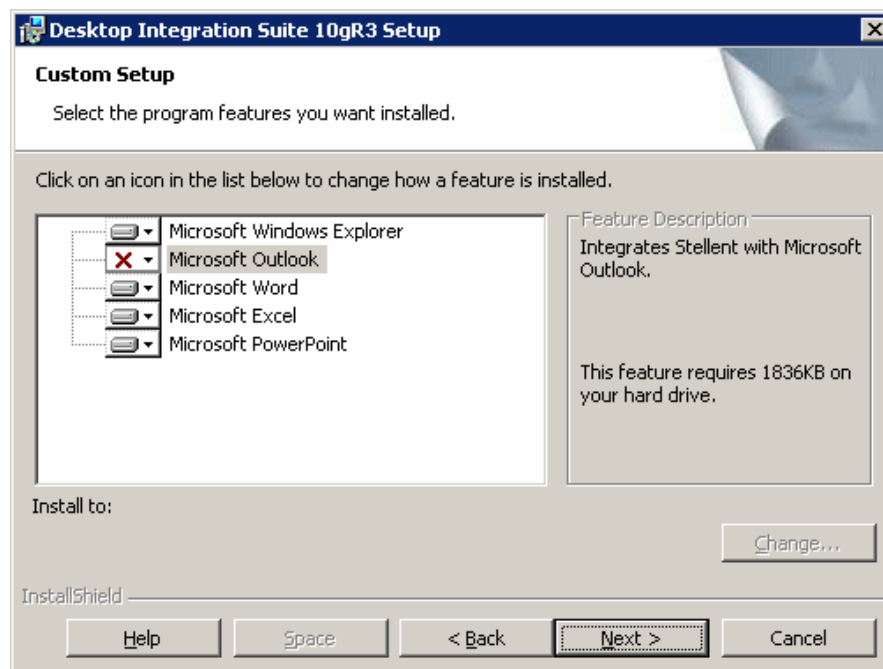
By default, the software is installed to *C:\Program Files\Oracle\Content Server\ Desktop Integration Suite*. If you want to install the software to a different folder, click the **Change...** button and point to a different destination.

After you have verified the applications to integrate with as well as the software installation location , click **Next** to continue, or **Cancel** to exit the installation process.

5. If any of the application that you want to integrate with Content Server are currently running, a warning may be displayed stating that some features of the Desktop Integration Suite will not be available until the affected applications are restarted. Click **Next** to continue.

6. Click **Install** to start the installation.

   All required files are copied.

> **Note:** When installing the Lotus Notes component, you may receive an error message stating that the *Notes.ini* file could not be found. If you receive this error, first complete the installation and then follow the instructions in Manually Configuring the Notes.ini File (see below).

7. After the installation has been completed, click **Finish** to exit the installation wizard.

MANUALLY CONFIGURING THE *Notes.ini* FILE

During installation of the Lotus Notes integration, changes are made to the *Notes.ini* file. If the installer is unable to make these changes, an error message is displayed.

To manually fix this error, complete the following steps:

1. Locate the *Notes.ini* file. You will find this file in the following location:

   • **Windows 2000/XP**: *[Lotus_Notes_App_Dir]\Notes.ini* (for example, *C:\Program Files\Lotus\Notes\Notes.ini*)

   • **Windows Vista**: *C:\Users\[User_Name]\AppData\Local\VirtualStore\ [Lotus_Notes_App_Dir]\Notes.ini* (for example, *C:\Users\jsmith\AppData\Local\ VirtualStore\Program Files\Lotus\Notes\Notes.ini*
   Please note that the Lotus Notes application directory also has a *Notes.ini* file, but this is not the file that needs to be modified.)

> **Note:** The AppData structure is hidden by default. You need to enable the option to view hidden folders in Windows Explorer.

Note: If multiple users are using a client computer running Windows Vista, then the *Notes.ini* file needs to be modified for each user.

Consult your Notes administrator if you have trouble finding the *Notes.ini* file.

2. Open the *Notes.ini* file in a text editor.

3. Look for the AddInMenus entry.

   ❖ If there is an AddInMenus entry, add STELNI.DLL to the end of the entry, separated by a comma:

   ```
   AddInMenus=FOOBAR.DLL,STELNI.DLL
   ```

   ❖ If there is no AddInMenus entry, add the following line to the end of the file:

   ```
   AddInMenus=STELNI.DLL
   ```

4. Save and close the *Notes.ini* file.

CONFIGURING SERVER CONNECTIONS AND METADATA

To complete the integration of Content Server with your desktop, you must establish a link between each client computer and each content server that you want to use for managing content. This link needs to be established only once, either from Windows Explorer, a desktop application, or your e-mail client. It is then established for all of the applications on that client computer.

This section covers the following topics:

❖ Adding a Server Connection (page 4-5)

❖ Determining the Server CGI URL Path (page 4-9)

❖ Setting Metadata To Be Remembered (page 4-9)

❖ Setting the Authentication Method (page 4-12)

Adding a Server Connection

Configuring the server and metadata varies slightly, depending on whether you are integrating Content Server with Microsoft Windows Explorer, an e-mail client, or a desktop application such as Microsoft Word or Excel.

You only need to add a server connection once. Any server connection made for one application will be available for the others.

Configuring metadata to be "remembered" (see page 4-9) applies only to the forms-based checkin in your desktop applications and e-mail clients. For folders-based checkin, metadata is handled through the Folders component.

Adding a New Server Connection
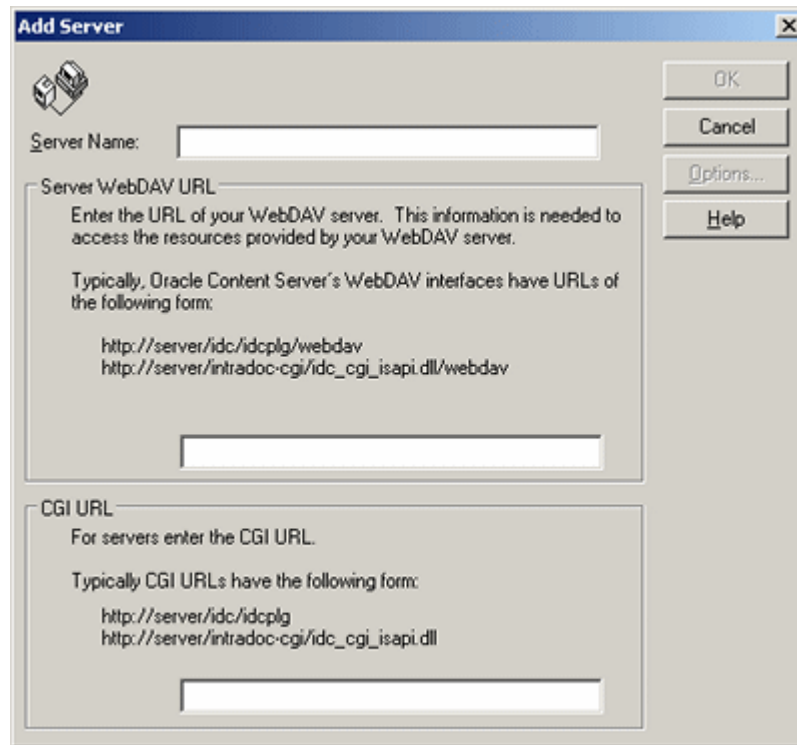
To add a new server connection, complete the following steps:

1. Open Windows Explorer.

2. Navigate to the bottom of the folders list. There will be an **Oracle Content Servers** item.

Figure 4-2   Oracle Content Servers in Windows Explorer

3. Right-click **Oracle Content Servers** and choose **Add Server** from the popup menu.

   The Add Server dialog box is displayed.

Figure 4-3   Add Server dialog

4. In the **Server Name** text box, enter the name you would like to display for the server in the Content Server folder hierarchy in Windows Explorer or your e-mail client.

5. In the text box under **Server WebDAV URL**, enter the web server URL.

    A URL is automatically inserted using the name you specified in the Server Name text box. You can also copy and paste one of the sample URLs provided.

6. In the text box under **CGI URL**, enter the CGI URL.

    A URL is automatically inserted using the name you specified in the Server Name text box. You can also copy and paste one of the sample URLs provided.

7. You can click the **Options...** button to open the Server Options dialog, where you can set the metadata to be remembered as well as the authentication method (see pages 4-9 and 4-12, respectively).

8. Click **OK**.

Configuring a Content Server in Your E-Mail Client

To configure a content server in your e-mail client, complete the following steps:

1. Open the Email Checkin Settings dialog box as follows:

   ❖ In Microsoft Outlook, click **Tools—Email Client Integration Settings**.

   ❖ In Lotus Notes, click **Actions—Email Client Integration Settings**.

2. Click **Edit Server List** to open that dialog box.

3. Click **New** to open the Add Server dialog box.

4. In the **Server Name** text box, enter a name for the server you are about to configure (you can use a user-friendly name).

5. In the text box under **Server WebDAV URL**, enter the web server URL.

   A URL is automatically inserted using the name you specified in the Server Name text box. You can also cut and paste one of the samples provided.

6. In the text box under **CGI URL**, enter the CGI URL.

   A URL is automatically inserted using the name you specified in the Server Name text box. You can also cut and paste one of the samples provided. (If you are not sure about the CGI URL, see Determining the Server CGI URL Path on page 4-9 for more information.)

7. You can click the **Options...** button to open the Server Options dialog, where you can set the metadata to be remembered as well as the authentication method (see pages 4-9 and 4-12, respectively).

8. Click **OK**.

Configuring a Content Server in a Desktop Application

To configure a content server in a desktop application, complete the following steps:

1. In the desktop applications, click **File—Open** to open the Select Content dialog box.

2. Click the **Server** tab.

3. Opposite the Server drop-down box, click the server icon (🌐) to open the **Edit Server List** dialog box.

4. Click **New** to open the Add Server dialog box.

5. In the **Server Name** text box, enter a name for the server you are about to configure (you can use a user-friendly name).

6. In the text box under **Server WebDAV URL**, enter the web server URL.

   A URL is automatically inserted using the name you specified in the Server Name text box. You can also cut and paste one of the samples provided.

7. In the text box under **CGI URL**, enter the CGI URL.

   A URL is automatically inserted using the name you specified in the Server Name text box. You can also cut and paste one of the samples provided. (If you are not sure about the CGI URL, see Determining the Server CGI URL Path on page 4-9 for more information.)

8. You can click the **Options...** button to open the Server Options dialog, where you can set the metadata to be remembered as well as the authentication method (see pages 4-9 and 4-12, respectively).

9. Click **OK**.

Determining the Server CGI URL Path

Integrating Content Server with your e-mail client or desktop application entails configuring the content server. If you are using a regular server, you will use the CGI URL path for the server.

To determine the server CGI URL path, complete the following steps:

1. Log into the content server, and navigate to the search page.

2. In the browser address bar, select and copy the search page URL from the beginning up to, but not including, the question mark (?). This is the CGI URL path.

3. Paste this URL into the CGI URL field in the Add Server dialog box. (See Adding a Server Connection on page 4-5.)

Setting Metadata To Be Remembered

When you add a server connection that allows you to manage content from a particular server from Windows Explorer or a desktop application, you can select metadata to be "remembered" each time you check in a content item.

As a result, at each check-in, the metadata values you used at the last check-in will pre-populate the remembered metadata fields (assuming the values are available). If you enter new values in the metadata fields, the new ones will be remembered the next time. You can select which metadata fields will be remembered in this way.

You can set the metadata when adding a new server, from a desktop application, or your e-mail client.

To set the metadata that should be remembered, complete the following steps:

1. Open the Server Options dialog.

   ❖ When adding a new server, click the **Options...** button in the Add Server dialog.

   ❖ From a desktop application:

      a. Click **File—Open** to open the Select Content dialog box.

      b. Click the **Server** tab.

      c. Opposite the Server drop-down box, click the server icon ( ) to open the **Edit Server List** dialog box.

      d. Select the Server you want to set remembered metadata for and click **Edit**.

      e. In the Edit Server dialog box, click **Options** to open the Server Options dialog box.

   ❖ From an e-mail client:

      a. In Microsoft Outlook, click **Tools—Email Client Integration Settings**. In Lotus Notes, click **Actions—Email Client Integration Settings**.

      b. Click **Edit Server List** to open that dialog box.

      c. Select the server you want to select "remembered" metadata for and click **Options**.

2. Open the **Remember Metadata Fields** tab.

Figure 4-4   Remember Metadata Fields tab in Server Options dialog
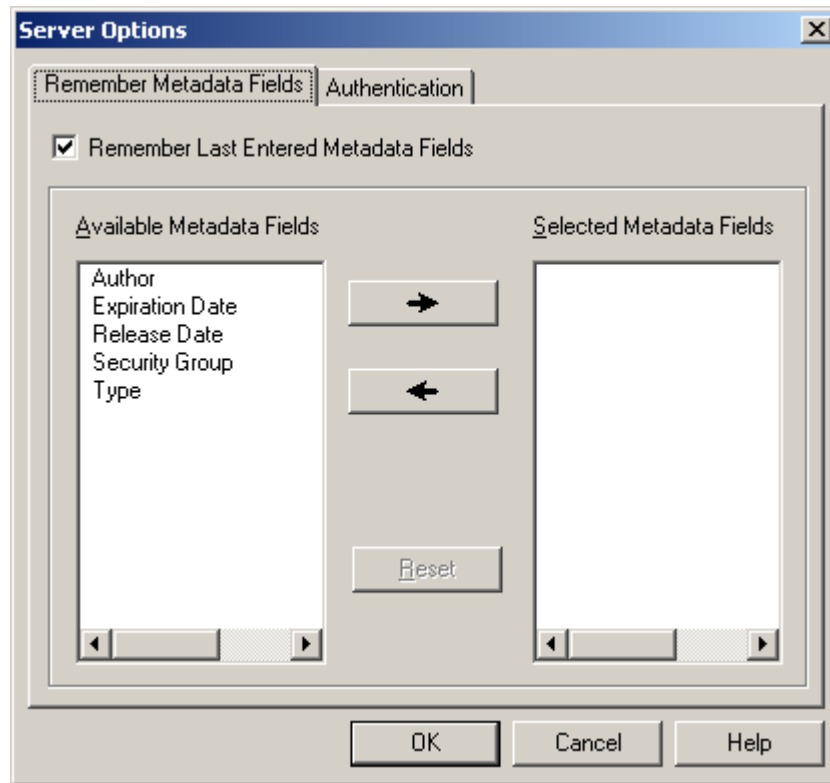
You set the value of the metadata fields when you check content into the content server.

3. Select the metadata fields to be remembered when you check content into the content server. Whatever values are set for these metadata fields for a particular check-in will automatically be used the next time you check in a content item.

    ❖ To use one or more fields, select each field to use under "Available Metadata Fields" and click the right arrow.

        Each field you select displays under "Selected Metadata Fields."

    ❖ To no longer use one or more selected metadata fields, select each field under "Selected Metadata Fields" and click the left arrow.

        Each field you selected displays under "Available Metadata Fields."

4. Click **OK** to return to the Server dialog box.

Before you edit or delete a server connection from the Edit Server dialog box, all content items currently checked out of that content server should be checked back in to ensure that any changes you have made to those content items are retained.

Setting the Authentication Method

When you create a connection to a server, your server options include the ability to set the authentication method (i.e., the method used by users to log on).

Typically, the authentication method will be set up by the system administrator and should not be changed.

To set the authentication method, complete the following steps:

1. Click **File—Open** to open the Select Content dialog box.

2. Click **Server** to open that tab.

3. Opposite the Server drop-down box, click the server icon (🐾) to open the **Edit Server List** dialog box.

4. Select the server you want to set the authentication method for and click **Options**.

5. In the Server Options dialog box, click the **Authentication** tab.

Figure 4-5   Authentication tab in Server Options dialog
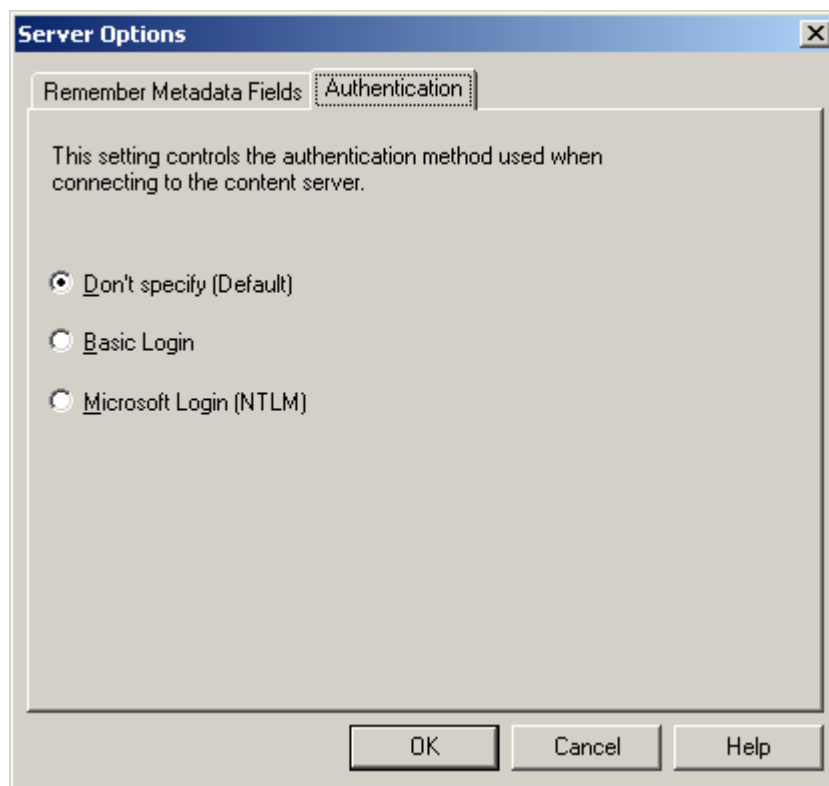
6. Select the authentication method you want to use.

The default setting is whatever has been set up for your content server. If you select **Microsoft (NTLM)**, you are using NTLM security. In that event, your user name and password are automatically supplied when you click the server, so you may not be prompted for login information.

7. Click **OK**.

UNINSTALLING DESKTOP INTEGRATION SUITE

You can uninstall the Desktop Integration Suite software completely, or uninstall one or more individual components, from any client computer at any time.

Uninstalling Desktop Completely

To completely uninstall the Desktop Integration Suite software from a client computer, complete the following steps:

1. Open Windows Control Panel.

2. Click **Add or Remove Programs**.

3. Select **Oracle Content Server - Desktop Integration Suite**.

4. Click **Remove** to start the Desktop Integration Suite Uninstall wizard.

5. Click **Yes** when asked if you are sure that you want to remove the Desktop Integration Suite software from your computer.

   The software is removed from the client computer.

Uninstalling Individual Components

To uninstall individual Desktop Integration Suite components, complete the following steps:

1. Open Windows Control Panel.

2. Click **Add or Remove Programs**.

3. Select **Oracle Content Server - Desktop Integration Suite**.

4. Click **Change** to start the Desktop Integration Suite Install wizard.

5. Go through the installation procedure (see page 4-2) and unselect the application(s) that you no longer want to integrate with Content Server.

5

CONFIGURING WINDOWS EXPLORER

OVERVIEW

After Content Server is integrated with Microsoft Windows Explorer, the system administrator can complete the following steps to enhance the integration. These should be done before the server connections are configured.

❖ **(Required)** – Configure some administrative and user settings in Content Server, which you may have already completed during Folders component setup. See Configuring the Folders Functionality (page 5-2) for further details.

❖ **(Optional)** – Create a registry file to automate the process of connecting to one or more content servers after Content Server has been integrated on each user's desktop. When you add a server connection in this manner, the user is unable to delete the server connection. See Configuring Content Servers (page 5-2) for further details.

❖ **(Optional)** – Configure the default "Open" action to allow users to open a content item only in a WebDAV-compliant application instead of its associated application. This is also done through a registry file. See Default "Open" Action (page 5-3) for further details.

CONFIGURING THE FOLDERS FUNCTIONALITY

Client configuration is performed through the web browser interface of the folders features of Content Server.

Some system administration configuration settings must be set before you use Desktop Integration Suite.

See Chapter 7 (*Content Server Administration Notes)* for a number of system administrative configuration tasks related to Content Server's folders features.

CONFIGURING CONTENT SERVERS

You can add your content server connections by creating a registry file. Desktop Integration Suite supports the configuration of servers and settings by executing a registry file named **defaults.reg** in the installation program's directory. The file is not included as part of the standard installation files; you must create it.

Adding servers in a registry file automates the setup process by saving your users from setting up connections on their computers. When you add a server connection in this manner, the user cannot delete the server connection from their desktop.

Sample Registry File

The following is a sample registry file, with comments.

```
REGEDIT4
[HKEY_LOCAL_MACHINE\SOFTWARE\Oracle\Desktop\WebDAV\Servers\
Corporate]
"ServerURL"="http://corporate/cserver/idcplg/webdav"
```

(Where the display name of the server is "Corporate," and the WebDAV server URL is "http://corporate/cserver/idcplg/webdav.")

```
[HKEY_LOCAL_MACHINE\SOFTWARE\Oracle\Desktop\WebDAV\Servers\
Department]
"ServerURL"="http://department/intradoc-cgi/idc_cgi_isapi.dll/
webdav"
```

(Where the display name of the server is "Department" and the WebDAV server URL is "http://department/intradoc-cgi/idc_cgi_isapi.dll/webdav.")

```
[HKEY_LOCAL_MACHINE \SOFTWARE\Oracle\Desktop\Stellent ODMA
Client\Config\Corporate]
"HostCgiUrl"="http://corporate/cserver/idcplg"
"ServerAuth"=dword:00000000 "RememberMetaData"=dword:00000000
```

(Where the name of the server is "Corporate," and the CGI URL is "http://corporate/cserver/idcplg.")

Users will not be able to delete this server from the desktop (Windows Explorer, the e-mail client, or any desktop application).

If you would like the user to run the installer, use HKEY_CURRENT_USER instead of HKEY_LOCAL_MACHINE.

Using HKEY_LOCAL_MACHINE means that users cannot change the ServerAuth or RememberMetaData values because they won't have permission to change HKEY_LOCAL_MACHINE entries (unless a Windows policy is set to allow this, or the user is an administrator).

HKEY_LOCAL_MACHINE values override HKEY_CURRENT_USER values.

DEFAULT "OPEN" ACTION

Another option for the integration of Windows Explorer is to change the "Open" default action to allow users to open a content item only in a WebDAV-compliant application, instead of opening it in its associated application, which may be non–WebDAV-compliant. This is also done by means of the **defaults.reg** file. (If you create the file to configure WebDAV servers, you can simply add an entry to change the "open" default action.)

The user guide explains the Open option based on the default functionality. When the user selects Open from the popup menu, the content item is automatically checked out and opened in its associated application, regardless of whether the application is WebDAV-compliant or not. The user then edits the content item and checks it back into the content server, creating a new revision with each check-in.

You can change the default setting so the Open action is compatible only with WebDAV-compliant applications. However, using this option with non-WebDAV compliant applications may generate errors. For example, if a user tries to open content that is associated with a non-WebDAV compliant application, such as a text file that is associated with Notepad, an error may display. The content does not open and it remains checked into the content server. To check out the content, the user must then check it out

through the content server web browser interface or by selecting Check Out from the Folders popup menu.

When you change the default Open action, the content item is always managed by Content Server. Typically, each time a user saves a content item a new revision is created. Depending on the application, there may be instances where a new revision is created only when the user closes the content item, as well, and the content item is automatically checked back into the content server.

Desktop Integration Suite supports the configuration of WebDAV servers and settings by executing a registry file named **defaults.reg** in the installation program's directory. The file is not included as part of the standard installation files; it must be created.

Open Action Value in Registry File

```
[HKEY_LOCAL_MACHINE\SOFTWARE\Oracle\Desktop\WebDAV]
"OpenWithCheckout"=dword:00000001
```

The default "Open" action will check out and open the file in its associated application, which may not be WebDAV-compliant. To use the default, the last digit of the dword value must be set to **1**.

If you choose not to use the default, set the last digit of the dword value to **0** so that WebDAV-compliant applications are required when the user selects the "Open" option.

6

INTEGRATING ADOBE ACROBAT CAPTURE

OVERVIEW

When you integrate Content Server with Adobe Acrobat Capture, you can manage images in the content server from that application. After you have run the Desktop Integration Suite Installer, you must then configure Adobe Acrobat Capture to work with the content server.

You must have Adobe Acrobat Capture 3.0 or higher installed on the client machine. You must also have Internet Explorer 4.0 or higher installed but it doesn't have to be your default browser.

CONFIGURING ADOBE ACROBAT CAPTURE

You must configure Adobe Acrobat Capture in order to archive images to Content Server. To do this requires:

❖ Building a Workflow With an Archive Step (page 6-2)

❖ Submitting Files to the Workflow (page 6-3)

Building a Workflow With an Archive Step

To archive images in the content server you must first build a workflow with an archive step.

Follow these steps to build a workflow with an archive step:

1. In Acrobat Capture Assistant, click the **Configure** tab.

2. Click **Insert Workflow** (🦋) on the toolbar above the Configure pane.

3. Under Workflow in the Configure pane, enter a name for the workflow in the text box that appears.

4. Click the **Edit** box alongside the name to ensure that the workflow is enabled (the status light is red).

5. Click **Insert Steps** (✔) from the list to open the Insert Steps dialog box.

Figure 6-1   Insert Steps dialog
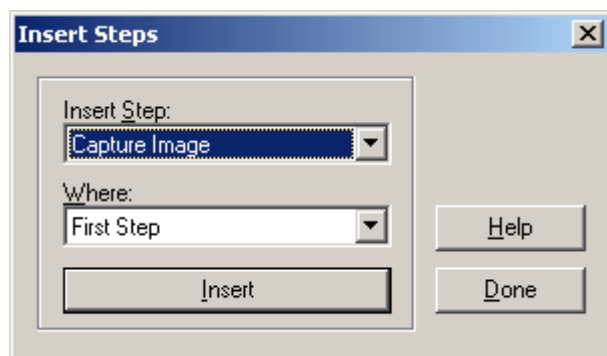
6. Select **Capture Image** from the Insert Step drop-down list, and **First Step** from the Where drop-down list. Click **Insert**.

   The Capture Image step is added to the workflow.

7. Select **Export to PDF** from the Insert Step drop-down list. The Where text box now displays the **After Capture Image** option. Click **Insert**.

   The Export to PDF step is added to the workflow.

8. Select **Archive File (PDF)** from the Insert Step drop-down list. The Where text box now displays the **After Export to PDF Image** option. Click **Insert**.

   The **Archive File Properties** dialog box is displayed.

Figure 6-2   Archive File Properties dialog

9. Under Document Management System, select **INTRADOC**.

10. Under File format, select **Other** and enter **PDF** as the file format.

11. Click **OK** to return to the Insert Steps dialog box. The Archive File (PDF) step is added to the workflow.

12. Click **Done**.

13. Select the Run box opposite the workflow. When the run box is enabled the status light is green.
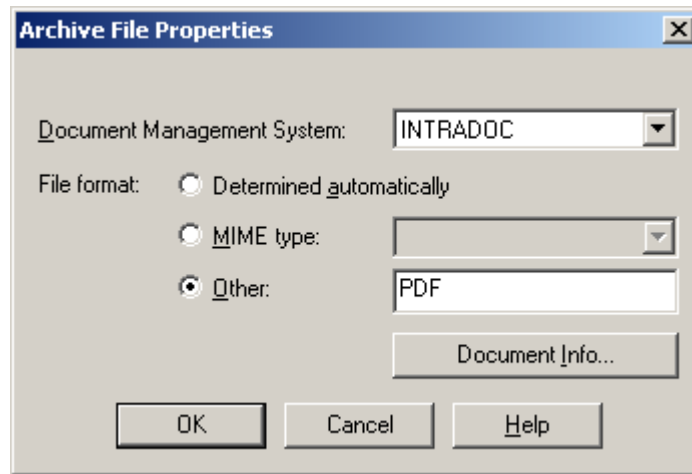
Submitting Files to the Workflow

After you have built a workflow with an archive step, you must then submit files to the workflow.

Follow these steps to submit files to the workflow:

1. Ensure that the **Run** box for the archive workflow is enabled (the status light is green).

2. Click the **Submit** tab.

3. Navigate to and select the file (or files) you want to include in the Workflow.

    To select the file(s), click the check box to the left of each file you want to submit.

    Files that you cannot submit to the archive Workflow are grayed out so that you can select only those files that are available for submission.

4. Select the workflow from the Target Workflow list.

5. Click **Submit to Workflow** to process the file. After some processing, the New Document dialog box displays. (The dialog box may initially display behind the Adobe Acrobat Capture dialog box.)

6. From the New Document dialog box, select a server and enter the document title, and then click **OK**.

   The Content Server check-in form is displayed.

7. Complete the content check-in form and click **Check In**.

CONTENT SERVER ADMINISTRATION NOTES

OVERVIEW

This chapter is intended for system administrators who have integrated Content Server with Microsoft Windows Explorer or an e-mail client.

The following topics are discussed:

❖ Initial System Administration Setup (page 7-2)

❖ System Administration Concepts (page 7-3)

❖ System Administration Reference (page 7-5)

❖ System Administration Tasks (page 7-12)

❖ EmailMetadata Component (page 7-15)

❖ RmaEmail Component (page 7-17)

Important: System administrators must complete some Folders component administrative tasks to work with the Content Server Folders functionality, which includes enabling a top-level system folder. See Initial System Administration Setup (page 7-2) for more information.

When you use the Content Server folders functionality, you also use the Folders component, which must be installed and enabled separately. For more information, see the Folders/WebDAV documentation for Content Server. You may also use the Collaboration Manager, and therefore view projects.

INITIAL SYSTEM ADMINISTRATION SETUP

When working with the Content Server folders functionality, you perform system administration tasks in the Folders component. This guide contains some of the Folders component administrative documentation for your reference, including notes on how these settings affect the Folders functionality. See the Folders/WebDAV documentation for complete instructions.

After you perform the tasks in the following table, users can begin interacting with the Content Server Folders features after they complete initial setup tasks as described in the *Desktop Integration Suite User Guide*.

Of the Folders component administrative tasks that can be performed for the Folders component, the options listed in the following table affect the Folders functionality. These are standard configuration options for the Folders component, and there are no special instructions for Folders.

Setting folder and file limits and entering the name of an inhibit field for metadata propagation is included as part of the Folders component installation, so these may have already been set. In addition, enabling top-level system folders is required as part of Folders component configuration. If you have not done so already, we highly recommend that you set system level metadata defaults if you use the Content Server folders functionality.

Task	Impact on Folders	Link to More Information
Setting folder and file limits (required)	Limits the number of folders and files that users can add.	Setting Folder and File Limits (page 7-12)
Disabling and enabling system folders (required)	Disables or enables top-level system folders. If a top-level system folder such as "Contribution Folders" is disabled, no one can interact with the folder until it is enabled again.	Disabling and Enabling System Folders (page 7-14)

Task	Impact on Folders	Link to More Information
Setting system level metadata defaults (recommended)	Sets system level metadata defaults that contain enough information to check content into the content server if no user metadata is set. When user default metadata is set, it overrides system default metadata.	Defining System Default Metadata (page 7-15)
Metadata propagation (optional)	If you propagate metadata through the Folders web browser interface, the information is reflected in the hierarchy in Folders.	See the Folders/WebDAV documentation.

SYSTEM ADMINISTRATION CONCEPTS

This section describes concepts and terms related to the Content Server Folders functionality. The following are covered next:

❖ WebDAV Client (page 7-3)

❖ Folders Functionality Overview (page 7-4)

WebDAV Client

A WebDAV client is a WebDAV-compliant application that can send requests and receive responses from the content server using the WebDAV protocol. Sample WebDAV-compliant applications include:

❖ Microsoft Word 2000 or higher

❖ Microsoft Excel 2000 or higher

❖ Microsoft PowerPoint 2000 or higher

When Content Server is integrated with Windows Explorer or an e-mail client, you can use the native application to check content into and out of a content server in the Content

Server folder hierarchy, regardless of whether the content is associated with a WebDAV-compliant application.

Folders Functionality Overview

Content Server's folders features provide an interface to the content server through Microsoft Windows Explorer or an e-mail client in the form of a folder hierarchy.

Figure 7-1   Windows Explorer interface to content servers
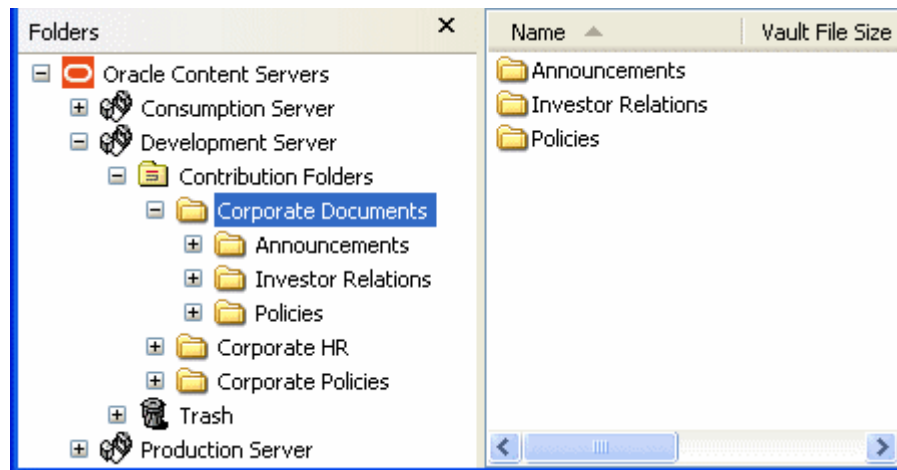
Consider the following points when using the folders features of Content Server:

❖ Content is viewable through a familiar interface.

❖ Users can apply default metadata to content items by checking them in through a particular folder.

❖ Each content server instance has a common set of folders. Any change to the folders is applied system-wide.

❖ There is one default system-level folder, called Contribution Folders. If you are using the Collaboration Manager, a "Projects" folder for this product may also display at the system level of the folders hierarchy.

❖ The system administrator can change the name of a system-level folder, but cannot delete it or add a custom system-level folder. Deleting a system-level folder disables it, but does not remove it from the system.

❖ Each folder in the hierarchy contains a unique "Collection ID" value. When you add content items to a folder, the "Collection ID" of the folder is assigned to the content.

Changing the Collection ID of a content item places it in a different location on the content server.

❖ The number of folders and number of files in each folder can be limited by the system administrator so that folder functions do not affect system performance.

SYSTEM ADMINISTRATION REFERENCE

This section describes pages that are used to configure folders and set user options, which must be performed as part of the initial Folders setup. See Initial System Administration Setup (page 7-2) for more information.

The following topics are discussed in this section:

❖ Virtual Folder Administration Configuration Page (page 7-5)

❖ System Folder Configuration Page (page 7-7)

❖ System Default Information Field Configuration Page (page 7-8)

❖ Information Field Inherit Configuration Page (page 7-10)

Virtual Folder Administration Configuration Page

The Virtual Folder Administration Configuration page is used to limit the number of folders and files that can be added using the web browser interface or Folders. It also provides access to the other Folder system configuration pages. To access this page, click the **Folder Configuration** link in the Administration tray from the content server web browser interface.

Figure 7-2   Virtual Folder Administration Configuration page

Feature	Description
Maximum Folders Per Virtual Folder field	Sets the maximum number of folders that any user can define: ❖ In the Folders component, if a user attempts to define more than this number of virtual folders, the **Save** command will return an error message. ❖ In Folders, an error message displays when the maximum number is reached and the user selects **New Folder** on the popup menu that displays.
Maximum Content Per Virtual Folder field	Sets the maximum number of files that any virtual folder can contain.
Update button	Applies the changes to the system.
Export Archive button	Exports the folder hierarchy as an archive file.

| Feature	Description
Import Archive button and field	Imports the specified folder archive. When you import a folder archive file, all current folders are removed from the content server and replaced by the imported hierarchy.
Browse button	Enables you to select the folder archive file you want to import.
System Folder Configuration button	Displays the System Folder Configuration Page (page 7-7).
System Default Information Field Configuration button	(Appears only if the system default metadata option is enabled.) Displays the System Default Information Field Configuration Page (page 7-8).
Local Folders button	Displays the Local Folders page. This does not affect Content Server Folders.
Information Field Inherit Configuration button	Displays the Information Field Inherit Configuration Page (page 7-10).

System Folder Configuration Page

The System Folder Configuration page is used to enable and disable system-level virtual folders. You may see only the top-level "Contribution Folders" system folder display, or you may see additional folders as well. For example, if you are using Collaboration Manager, you may also see a Projects folder.

To access this page, do one of the following from the content server web browser interface:

❖ In the Administration tray, expand the Folder Configuration Link and click the **System Folder Configuration** link.

❖ Click the **System Folder Configuration** button on the Virtual Folder Administration Configuration Page (page 7-5).

Figure 7-3 System folder configuration page
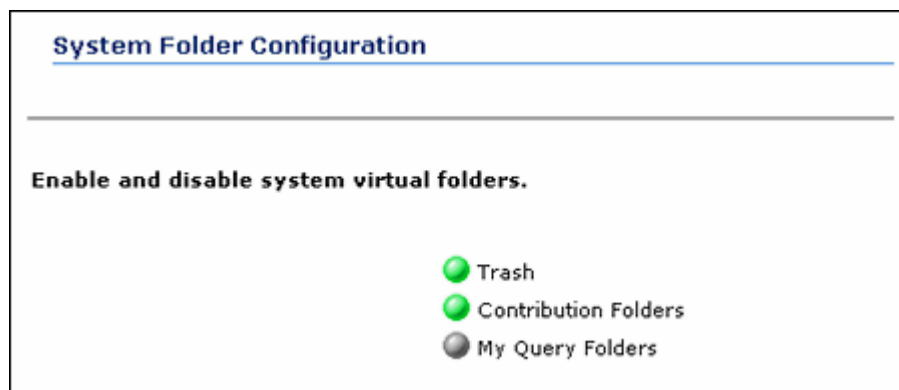
Clicking an icon displays the associated system virtual folder and enables or disables the folder:

❖ Green ( ) = Enabled. Users see the folder in the Content Server folder hierarchy and in the Exploring pages through the web browser interface.

❖ Gray ( ) = Disabled. Users do not see the folder in the Content Server folder hierarchy or in the Exploring pages through the web browser interface.

System Default Information Field Configuration Page

The System Default Information Field Configuration page is used to set system default metadata for folders. To access this page, do one of the following from the content server web browser interface:

❖ In the Administration tray, expand the Folder Configuration Link and click the **System Default Information Field Configuration** link.

❖ Click the **System Default Information Field Configuration** button on the Virtual Folder Administration Configuration Page (page 7-5) to open.

Figure 7-4   System Default Information Field configuration page

Feature	Description
Information fields	Define the metadata values that will be applied to content checked in through a virtual folder if values are not already defined for the folder or by the user.
	These metadata values are applied only on initial check-in. These settings do not affect revisions to existing content.
	Idoc Script can be used in any of the information fields.
	Although the Release Date field is required, the content server will automatically use the current date and time if this field is left blank.
Update button	Applies changes to the system defaults.
Reset button	Resets the fields to the last saved values.

Information Field Inherit Configuration Page

The Information Field Inherit Information page is used to select which metadata values will be propagated from a folder to its subfolders and content items.

To access this page, do one of the following from the content server web browser interface:

❖ In the Administration tray, expand the Folder Configuration Link and click the **Information Field Inherit Configuration** link.

❖ Click the **Information Field Inherit Configuration** button on the Virtual Folder Administration Configuration Page (page 7-5).

You must set these values on the Information Field Inherit Configuration page shown below, and not through Folders. See the *Folders and WebDAV Administration Guide* for complete information about metadata propagation.

Figure 7-5   Information Field Inherit Configuration page

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

SYSTEM ADMINISTRATION TASKS

This section describes the tasks related to working in Folders that a system administrator can perform.

System administrators must complete some Folders component administrative tasks to use Folders, including enabling a top-level system folder. See Initial System Administration Setup (page 7-2) for more information.

When you use the Content Server folder functionality, you also use WebDAV Server and Folders component, which are implemented as custom components. For more information, see the *Folders and WebDAV Administration Guide*. You may also use the Collaboration Manager, and therefore view Projects. See the *Collaboration Manager Administration Guide.*

The following topics are discussed in this section:

❖ Setting Folder and File Limits (page 7-12)

❖ Disabling and Enabling System Folders (page 7-14)

❖ Defining System Default Metadata (page 7-15)

Setting Folder and File Limits

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

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

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

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

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

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

1. Log in to the content server as an administrator.

2. Open the **Administration** tray.

3. Click the **Folder Configuration** link.

   The Virtual Folder Administration Configuration page (see page 7-5) is displayed.

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

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

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

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

6. Click **Update**.

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

Disabling and Enabling System Folders

Use the following procedures to disable and enable a system-level virutla folder. This applies to both the web browser and Folders.

Use the web browser interface to disable and enable system-level folders, such as "Contribution Folders" or "Projects."

Disabling a System Folder

1. Log into the content server as an administrator.

2. Open the **Administration** tray.

3. Expand the **Folder Configuration** link.

4. Click the **System Folder Configuration** link.

5. The System Folder Configuration Page (page 7-7) is displayed.

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

7. The folder is disabled. Users will not be able to see the disabled folder in the web browser interface or through Folders.

Enabling a System Folder

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

1. Log into the content server as an administrator.

2. Open the **Administration** tray.

3. Expand the **Folder Configuration** link.

4. Click the **System Folder Configuration** link.

   The System Folder Configuration Page (page 7-7) is displayed.

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

6. The folder is enabled and the Exploring page for the folder is displayed. Users will be able to see the enabled folder in the web browser interface and through Folders.

Defining System Default Metadata

Use this procedure to define the system default metadata. Doing so is highly recommended when you use Folders. These defaults will be applied to any content checked into a folder only if a value is not defined for the folder or by the user.

Users should still set their own default metadata to ensure that content items do not all have the same metadata.

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

1. Log into the content server as sysadmin through a web browser.

2. Open the **Administration** tray.

3. Expand the **Folder Configuration** link.

4. Click the **System Default Information Field Configuration** link.

    The System Default Information Field Configuration Page (page 7-8) is displayed.

5. Specify the default values to be applied to content upon checkin.

6. Click **Update**.

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

EMAILMETADATA COMPONENT

The EmailMetadata component automatically assigns e-mail metadata for Microsoft Outlook message files and Lotus Notes message files checked into a content server. This is useful for contributing e-mail content using Content Server Folders in Microsoft Outlook or Lotus Notes. The EmailMetadata component can be installed either through the Admin Server user interface or via the Component Wizard.

When a Microsoft Outlook message (MSG) or Internet Mail Message (EML) is checked into a content server, the EmailMetadata component extracts these message fields: From, To, Subject, CC, Sent Date, and Received Date. This information is then used to populate empty e-mail fields for the checked in content item. Specifically, this component assigns the xEmailTo, xEmailFrom, xEmailSubject, xEmailCC, xPublicationDate, and xReceivedDate e-mail fields.

To use the EmailMetadata component on Content Server 6.*x*, you must change the CLASSPATH variable in the **bin/intradoc.cfg** file to ensure that it references the jars in the EmailMetadata/lib directory. Restarting the content server is also required.

Example (Windows):
```
CLASSPATH=$COMPUTEDCLASSPATH;C:/CServer/idcm1/custom/EmailMetadata/lib/mail.jar;
C:/CServer/idcm1/custom/EmailMetadata/lib/poi-3.0-rc4-20070503.jar
```

Example (Unix):
```
CLASSPATH=$COMPUTEDCLASSPATH:/cserver/idcm1/custom/EmailMetadata/lib/mail.jar:
/cserver/idcm1/custom/EmailMetadata/lib/poi-3.0-rc4-20070503.jar
```

The EmailMetadata component uses the file extension for processing. Other file formats that use the MSG or EML extension (formats other than Microsoft Outlook, or Lotus Notes) will be processed by the EmailMetadata component, but their metadata will not be extracted.

EmailMetadata does not set up metadata fields on the content server; you must do so manually or by installing the RmaEmail component. See Adding E-Mail Metadata Fields Manually (page 3-5).

The EmailMetadata component does not override the e-mail fields (EmailFrom, EmailTo, EmailCC, etc.) that a user enters on the checkin form when checking a mail item in with Microsoft Outlook or Lotus Notes.

The EmailMetadata component interprets e-mail message header fields using the system default character set of the content server. For example, the metadata extracted from a Japanese e-mail message may be garbled if the content server is configured to process e-mail messages using a Western European character encoding.

This behavior can be overridden by setting the EmailMetadataEncoding entry in the config.cfg configuration file. For example, setting 'EmailMetadataEncoding=sjis' would force the EmailMetadata component to use a Shift-JIS encoding when processing e-mail messages. The available encoding types depend on the particular JVM you are using.

Customizing and Regulating Field Lengths

The EmailMetadata component can be customized to meet the particular needs of your organization. By default the component will populate the following fields:

xEmailSubject	xEmailTo	xPublicationDate
xEmailFrom	xEmailCC	xReceivedDate

The EmailMetadata component automatically discovers the appropriate field lengths from the content server. If you want to regulate field lengths, you can customize the component to truncate values by editing the configuration HDA file 'emailmetadata_resources.hda' located in the \custom\EmailMetadata\resources directory of the content server. The EmailMetadata component will then limit the length of extracted e-mail metadata values to the lengths specified in the configuration HDA file.

❖ For MSG messages, limit field lengths by lowering the value in the MaxSize column of the EmailMetadataConversionMap ResultSet.

❖ For EML messages, limit field lengths by lowering the value in the MaxSize column of the EmailMetadataEMLConversionMap ResultSet.

The MaxSize value of each record determines the maximum length of the extracted text for that record's MetadataField. For example, to set the truncation length of the xEmailFrom field to 30, you would change the default value of -1 to 30. This would need to be done in both ResultSets for every record that specifies how to populate the xEmailFrom field. A value of -1 for any of the field lengths will instruct the component to discover the appropriate length from the content server (default value). A value of 0 instructs the component not to truncate.

After making any changes to the EmailMetadata configuration file, you must restart the content server for those changes to take effect.

If you install a new version of the EmailMetadata component, you will have to reapply your changes.

RMAEMAIL COMPONENT

The Records Manager Email (RmaEmail) component is an optional component and is typically used in conjunction with the Universal Records Management solution, which helps organizations manage their business records and therefore meet certain corporate compliance requirements.

If your server uses the RmaEmail component, you can check distribution lists into the content server: ones that already exist in Microsoft Outlook, Lotus Notes, or new ones you create. After the distribution list is checked in, you can edit it, as needed.

Please note the following if your content server is set up to use the RmaEmail component:

❖ The e-mail specific metadata fields are automatically added to the content server.

❖ After you check in the e-mail, the date fields (Publication Date and Receive Date) are locked and cannot be changed. However, you can change the other e-mail metadata values when you check an e-mail into the content server.

❖ Outlook VCard (.vcf) files are not checked into the content server.

❖ When you view an e-mail that is checked into the content server containing one or more attachments, the URL to the Info page for the most recent revision of each attachment displays at the bottom of the message. With the RM Email component, however, the URL to the Info page always Heading Text + Pages to the first revision, regardless of whether the content item has newer revisions.

8

ADDITIONAL STEPS FOR DOMINO ADMINISTRATORS

OVERVIEW

Lotus Domino administrators may need to perform additional steps to ensure users can successfully view and work with the Content Server Folders functionality in Lotus Notes e-mail.

There are two different issues during the Desktop install for Lotus Notes that can be addressed by the Domino Administrator.

❖ **Execution Control List (ECL)**

Issue: The user is prompted with Execution Security Alerts (ESA) during an "Enable Folders" operation.

The Domino Administrator can add the "Stellent Development/Stellent" user to the Administration ECL on the Domino server, and add a Policy Document to push that change automatically to their Notes users.

❖ **Design Elements in the Mail Database**

Issue: If Lotus Notes users do not have Designer rights (ACL) to the Notes database, they will not see a "Show Folders" check-box in the Email Checkin Settings dialog box. As a result, they will not be able to view Content Server folders inside Lotus Notes.

The Domino Administrator can add the Desktop design elements to a copy of the Standard Notes mail template, and push that to selected Notes users.

The following topics are discussed in this chapter:

❖ Creating ECL for Users (page 8-2)

❖ Creating an Explicit Policy and Assigning Users (page 8-7)

❖ Adding Folders Design (page 8-8)

CREATING ECL FOR USERS

Follow these steps to create an Execution Control List for the users:

1. Open the Lotus Administration program and select the Settings tab.

Figure 8-1   Lotus Administration program
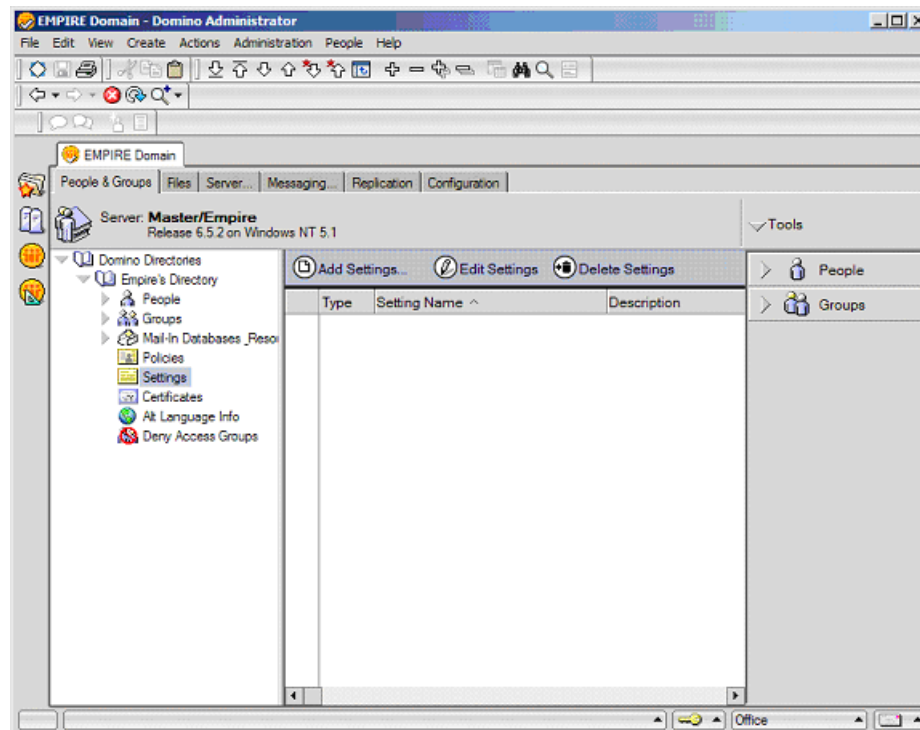
2. From the Add Settings menu select Security.

3. Answer Yes to the Security Warning.

4. Add a name and description, then select **Save & Close**.

5. Double click on the document you just created to open it.

Figure 8-2   Security settings
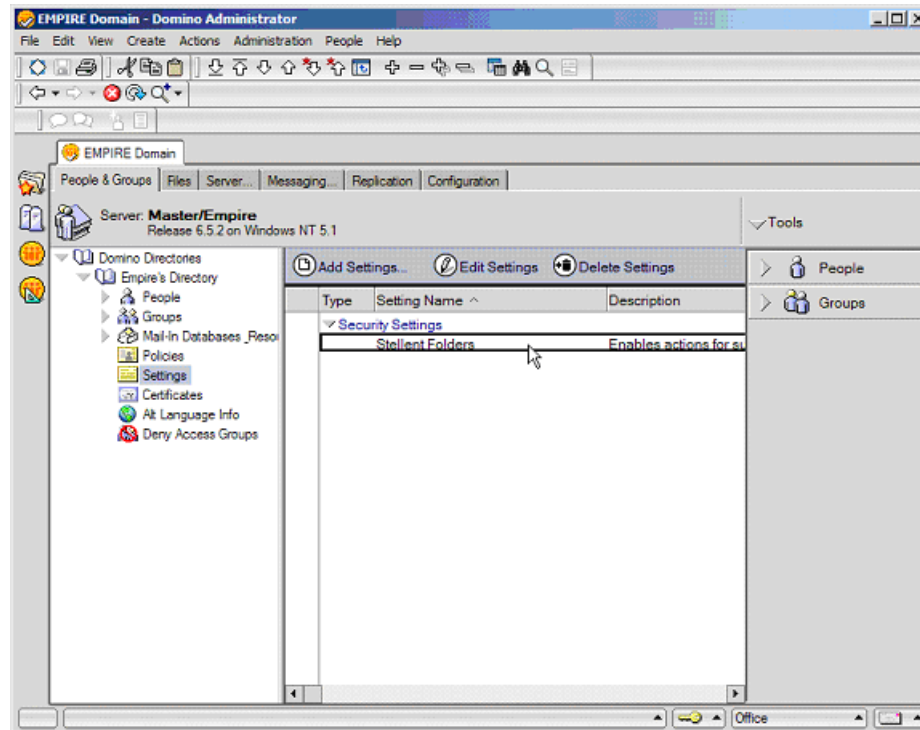
6.   Double click in the document to place it in Edit Mode.

7.   Select **Execution Control List** and then click **New**.

**Figure 8-3**   Execution Control List dialog
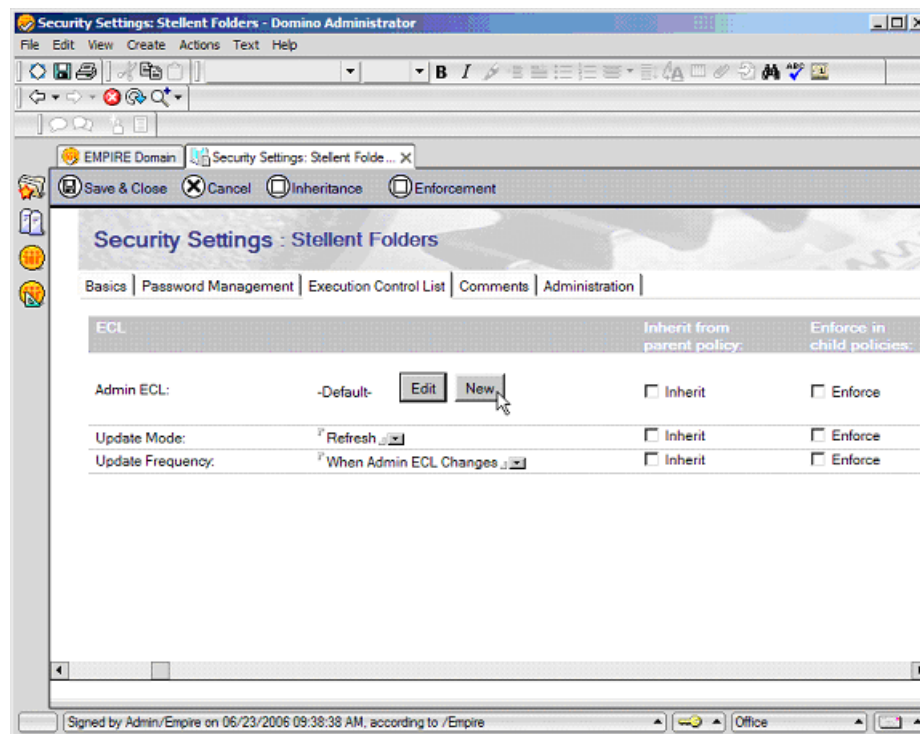
8.   Create a name for this document. In this example, for clarity, we gave it the fully qualified name of the Stellent Development signer.

9.   On the Execution Control List, click **Add**.

Figure 8-4   Execution Control List
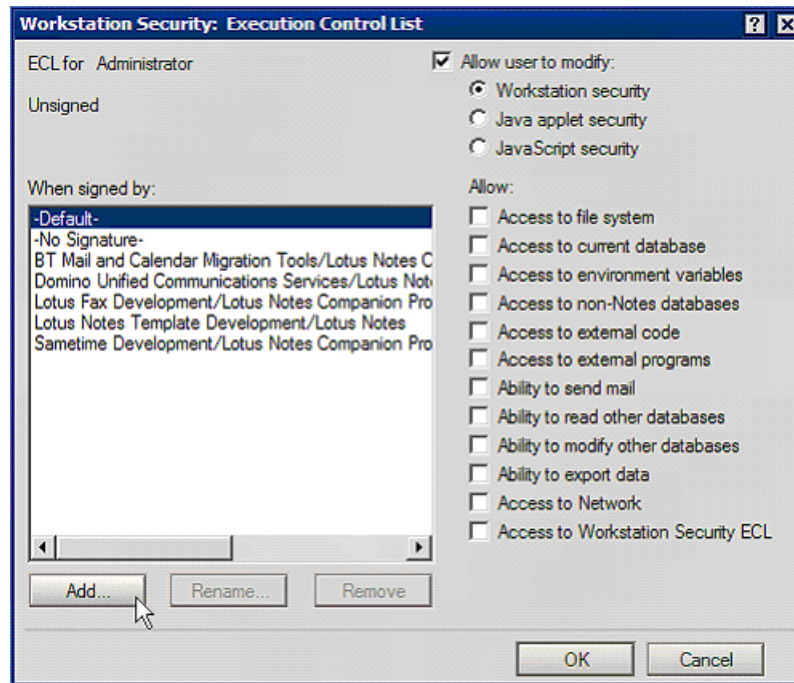
10. Enter the Stellent Development signer "Stellent Development/Stellent" and click **OK**.

11. Add permissions for Access to the current database, environment variables, external code, external programs, read other databases, and modify other databases, then click **OK**.

Figure 8-5   Security permissions
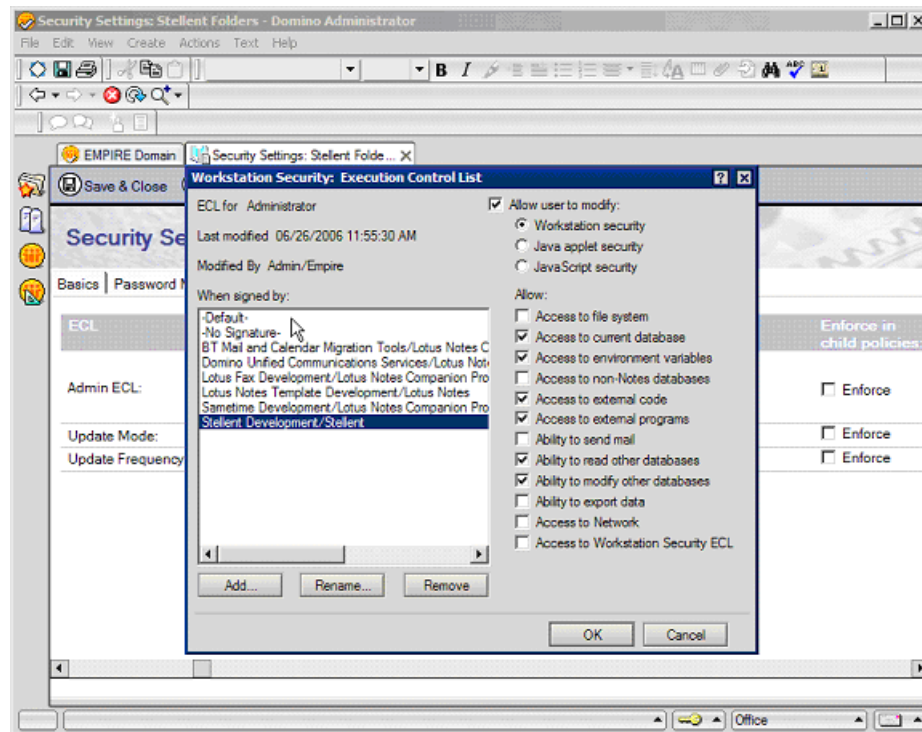
12. Create a Notes Certifier for the /Stellent organization by expanding the Certification menu and selecting **Cross Certify Key**.

13. Select your server's certifier method and click **OK**.

14. Enter your Certifier Password (empire).

15. For the Cross Certificate, enter the Subject name, Public key, and Expiration date. For example:

    ❖ Subject name: /Stellent

    ❖ Public key: 1443B RAD7Q Q2EZK XY47N BPQJT 184A3

    ❖ Expiration date: 06/23/2016 12:49:16 PM

Figure 8-6 Cross Certificate details
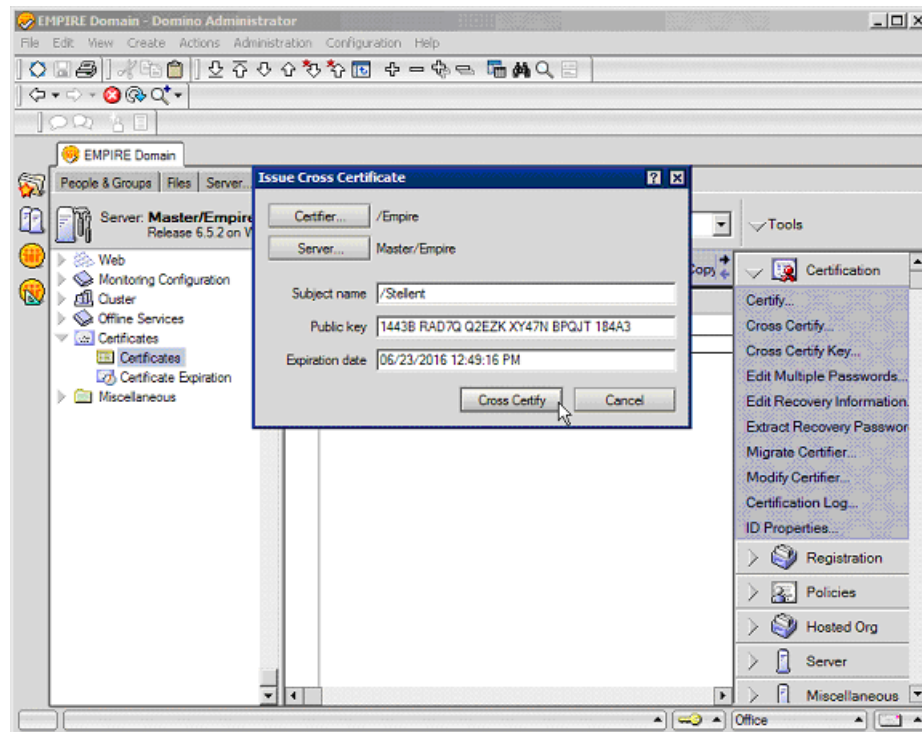
When done, click **Cross Certify** and then select **Save & Close**.

16. Click **No** when prompted to "certify another with the current certifier."

CREATING AN EXPLICIT POLICY AND ASSIGNING USERS

Follow these steps to create an Explicit policy and assign users:

1. Navigate to the Policies tab and click **Add Policy**.

2. Click **Yes** on the creating policies warning.

3. Create an Explicit policy with the name "/Oracle Desktop Integration" and then click the drop down button next to the Security field.

4. Select the "Oracle Content Servers" security document (previously created) and click **OK**.

5. Select **Save & Close**.

6. Add this Policy to the users that will have Desktop Integration. Select the People tab, then a user, then click **Edit Person**.

7. In the Person document, select the Administration tab and click the drop down button next to the Assigned policy field.

8. Select the "/Oracle Desktop Integration" policy document (previously created) and click **OK**.

9. Select **Save & Close** to save the changes to the Person document.

ADDING FOLDERS DESIGN

This section discusses the Lotus Notes / Folders architecture, presents the steps to add the Folders Design in a mail template, and how to distribute the new mail template to e-mail users. It covers the following topics:

❖ Lotus Notes / Folders Architecture (page 8-8)

❖ Installing Folders Design into a Mail Template (page 8-9)

❖ Distributing to Email Users (page 8-13)

Lotus Notes / Folders Architecture

When the installer is run on the user's machine, the file StellentFoldersTemplate.ntf is placed in the Lotus Notes Data directory. This template contains the Design Documents for the Content Server Folders functionality, and is signed by the user "Stellent Development/Stellent". Each Design Document is marked to inherit from the design template named "StellentFoldersTemplate", and the template file is labeled as a master template with the same name.

This architecture allows a Notes User with Designer rights to their Mail database to install the Folders changes without intervention by a Domino Administrator. Since the Design Documents are marked to inherit from a different template than the mail template, normal changes to the mail template (for example, updates from Lotus) will still work without disrupting the Content Server Folders functionality. If desired, the StellentFoldersTemplate can be placed on the Domino Server, and any changes from the content server can be automatically distributed.

If mail users do not have Designer rights, or if it is preferred to add the Folder Design for the users, then the Domino Administrator can add the Folders Design to a copy of the standard Lotus e-mail template and convert a user's mail file to use this new template.

Installing Folders Design into a Mail Template

1. On a workstation with the Notes Admin client, install the Desktop Integration software.

2. Using the Lotus Notes client, add the default mail template to your workspace (select **Database—Open**).

Figure 8-7   Default mail template addition
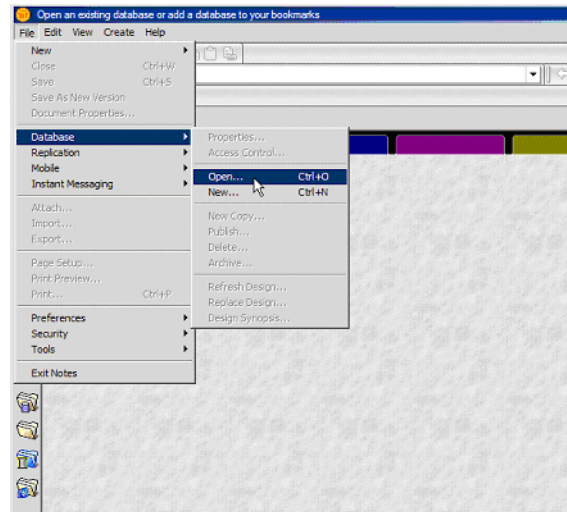
3. On the Open Database dialog, click **Browse**.

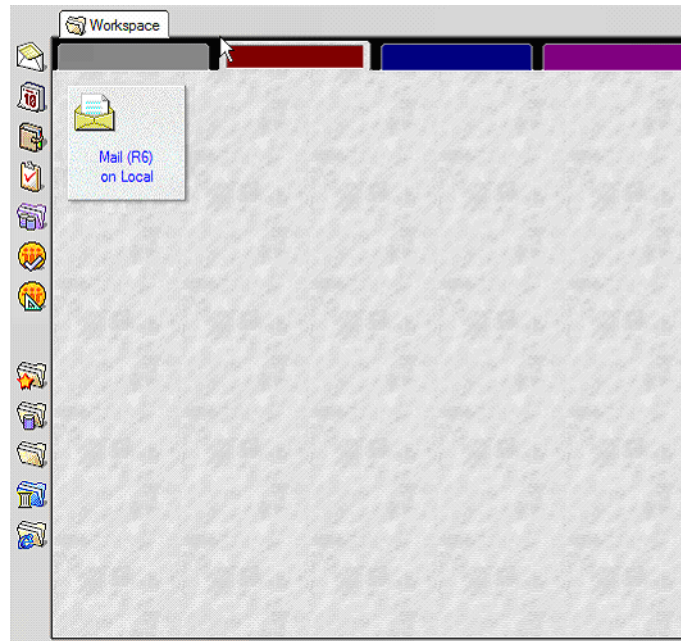4. Select **Notes Template Files** from the "Files of type" drop-down list.

Figure 8-8   Files drop-down list
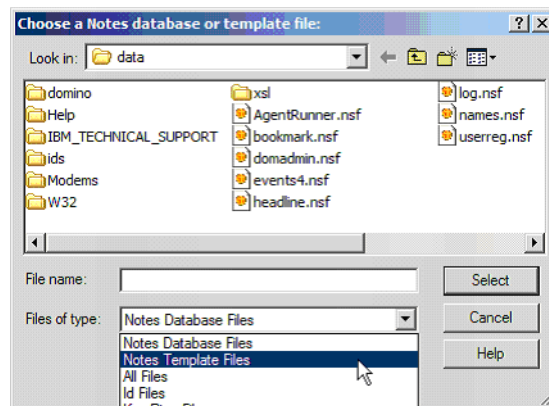
5. Choose an existing mail template file (e.g., mail6.ntf) and click **Select**.

6. On the Open Database dialog, click **Open** to open the template file.

7. Close the template you just opened. This leaves the icon on your workspace.

Figure 8-9 Icon in workspace

8. Right click the icon and select **Database—New Copy**.

**Important:** Select Database, not Replication; create a New Copy, not a replica.

Important: Do not use the file system to make a copy of the file.

9. Enter a new Title and new File name (e.g., newmail6.ntf) for the template. and then click **OK**. This file name is used again in later steps.

10. On your workspace, right-click on the new icon and change the template name by right clicking and choosing **Database—Properties**.

Figure 8-10   Changing the template name
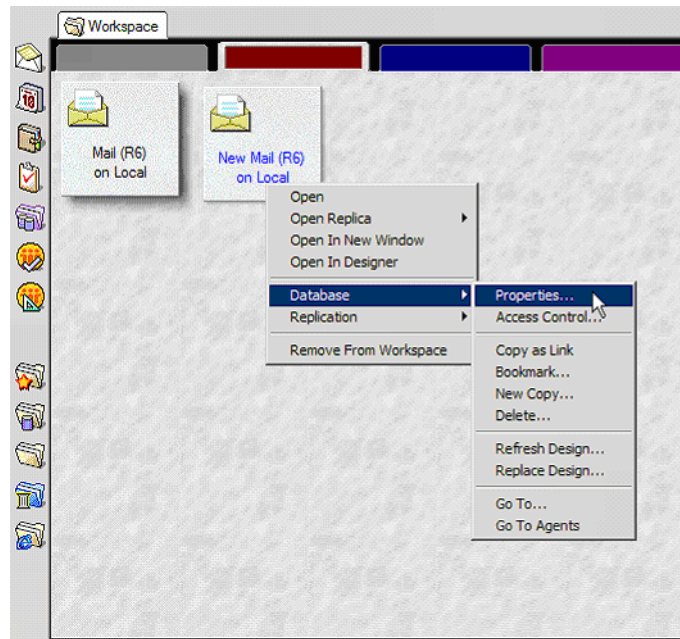
11. Select the Design Tab. Change the Template name (e.g., NewStdR6Mail) and click the associated check-mark button to add the new template. Close the dialog.

Figure 8-11 Check-mark buttons
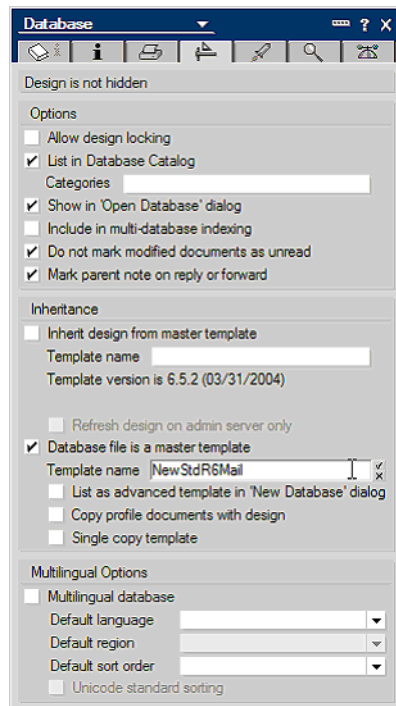
12. Open the template by double clicking it and enable the Content Server Folders by selecting **Actions—Email Client Integration Settings**.

13. On the Email Checkin Settings dialog, enable the **Show Folders** option and click **OK**.

14. On the Create Cross Certificate dialog, click **Yes**.

Figure 8-12 Create Cross Certificate dialog
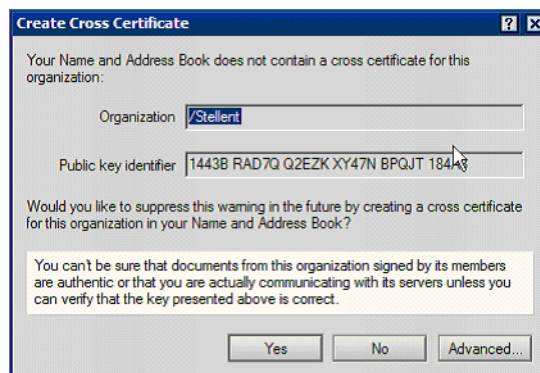
15. If you have not already pushed out the ECL policy, select **Start trusting the signer to execute this action** and click **OK** for the following Execution Security alerts:

- Stellent... Access to environment variables.

- Stellent... Access to external code.

- Stellent... Ability to read other databases.

- Stellent... Access to current database.

- Stellent... Ability to modify other databases.

16. When prompted to close and reopen the database, click **OK**.

17. Select **Start trusting the signer to execute this action** and click **OK** for the following Execution Security Alert:

- Stellent... Access to external programs.

Distributing to Email Users

Now you have a working Folders in a new mail template. To distribute this to email users, you can use the Domino convert tool:

1. Create a new replica for the database and click **OK** (to place the new template on your Domino server).

   ❖ Be sure to select Server not Local.

   ❖ The file name must match the name used in the previous steps (e.g. newmail6.ntf).

Figure 8-13   Domino convert tool
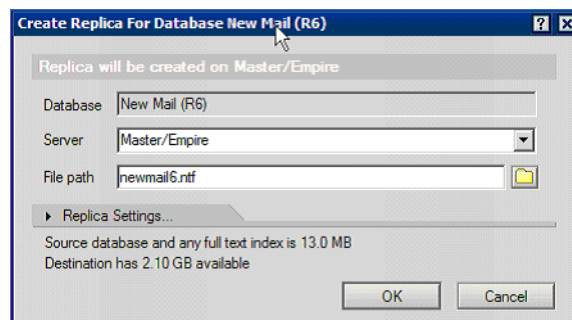
2. Start the Domino Admin client. Select the Server tab, then the Status tab, then the Tools drop down menu. In the Task drop-down click **Start**.

Figure 8-14 Domino Admin client
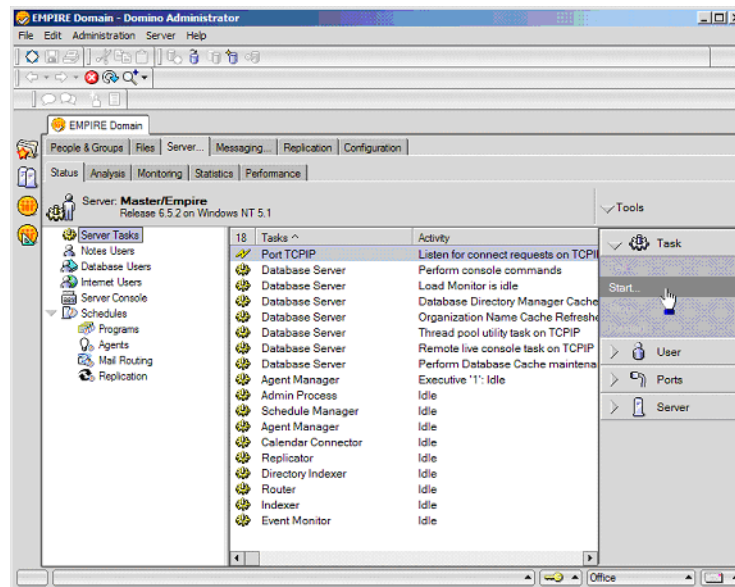
3. On the Start new Task dialog, select the Converter task, enable "Select advanced options" and click **Start Task**.

4. On the Lotus Notes dialog, enter the name of the new mail template file, and the file name and path for the mail database you wish to convert. Click **OK**.

   ❖ The file name must match the name used in the previous steps (e.g. newmail6.ntf).

   ❖ For path and filename of databases, this should be a user mail file.

The conversion will run on the Domino server. When the mail box is next opened, the Content Server Folders hierarchy are enabled.

CUSTOM INSTALLATION OPTIONS

OVERVIEW

The Desktop Integration Suite installers support a number of custom installation options that can help system administrators roll out the software:

❖ Command Line Operation (page A-1)

❖ Disabling Integrations (page A-2)

❖ Silent Roll-Outs (page A-3)

COMMAND LINE OPERATION

You can use a number of command line parameters to automate (part of) the installation process.

MSI Installer

You can use command line parameters for the MSI installer as follows:

```
msiexec /i "DesktopIntegrationSuite.msi" WORD=0 INSTALLDIR="c:\desktop"
```

The `/i` switch provides the name of the MSI package to be installed, and the `INSTALLDIR` the installation directory of the Desktop software. The double quotes are required only if the parameter value has spaces in them (for example "C:\Program Files\Desktop" as the installation directory), but using them for values without spaces will not hurt anything. See page A-2 for more information about the `WORD` parameter.

Setup.exe

The *Setup.exe* variety of the installer can be invoked from the command line as follows:

```
setup.exe /v"WORD=0 EXCEL=0 INSTALLDIR=\"e:\program files\desktop\""
```

The `/v` switch passes parameters to the MSI package. Please note the placement of the double quotes around the entire '/v' switch section. If any command line argument has spaces in it, then it must be embedded in double quotes, as in the INSTALLDIR property above. Please note the backslash (\) in front of the double quotes (as they are embedded within the double quotes for the '/v' switch).

Note: See below for more information about the `WORD` and `EXCEL` parameters.

DISABLING INTEGRATIONS

The Desktop Integration Suite installers provide a number of command-line options that enable you to disable specific software integrations. Normally, if the installer detects that an integration can be applied to existing software on the computer (Microsoft Word, PowerPoint, Excel, etc.), it will automatically attempt to install an integration. If you do not want an integration installed for a specific software product, you can disable that integration using these command-line switches:

- CAPTURE=0
- EXPLORER=0
- EXCEL=0
- NOTES=0
- OUTLOOK=0
- POWERPOINT=0
- VISIO=0
- WORD=0
- WORDPERFECT=0
- WORDPRO=0

Make sure that you use capital letters for the switch names. See above for examples of how to use these switches in command line operation.

Note: Switches are only used to disable software integrations; you do not need to use any switches to enable software integrations for applicatios that are found on the client computer.

SILENT ROLL-OUTS

The MSI installer enables system administrator to roll out the Desktop Integration Suite software to multiple client machines with the help of third-party tools such as SMS or netOctopus, which are capable of executing one executable on many machines. The MSI installer for the Desktop Integration Suite software supports a silent installation option that can easily be configured with SMS. The command to install the Desktop software silently is as follows:

```
msiexec /q /i "DesktopIntegrationSuite.msi" WORD=0 INSTALLDIR="c:\desktop"
```

B

THIRD PARTY LICENSES

OVERVIEW

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

❖ Apache Software License (page B-1)

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

❖ Zlib License (page B-4)

❖ General BSD License (page B-5)

❖ General MIT License (page B-5)

❖ Unicode License (page B-6)

❖ Miscellaneous Attributions (page B-7)

APACHE SOFTWARE LICENSE

```
* Copyright 1999-2004 The Apache Software Foundation.

* Licensed under the Apache License, Version 2.0 (the "License");

* you may not use this file except in compliance with the License.

* You may obtain a copy of the License at

*      http://www.apache.org/licenses/LICENSE-2.0

*
```

```
                        * Unless required by applicable law or agreed to in writing, software

                        * distributed under the License is distributed on an "AS IS" BASIS,

                         * WITHOUT WARRANTIES OR CONDITIONS OF ANY KIND, either express or implied.

                         * See the License for the specific language governing permissions and

                         * limitations under the License.
```

W3C® SOFTWARE NOTICE AND LICENSE

```
                        * Copyright © 1994-2000 World Wide Web Consortium,

                        * (Massachusetts Institute of Technology, Institut National de

                        * Recherche en Informatique et en Automatique, Keio University).

                        * All Rights Reserved.  http://www.w3.org/Consortium/Legal/

                        *

                        * This W3C work (including software, documents, or other related items) is

                        * being provided by the copyright holders under the following license. By

                        * obtaining, using and/or copying this work, you (the licensee) agree that

                        * you have read, understood, and will comply with the following terms and

                        * conditions:

                        *

                        * Permission to use, copy, modify, and distribute this software and its

                        * documentation, with or without modification, for any purpose and without

                        * fee or royalty is hereby granted, provided that you include the following

                        * on ALL copies of the software and documentation or portions thereof,

                        * including modifications, that you make:

                        *

                        *   1. The full text of this NOTICE in a location viewable to users of the

                        *      redistributed or derivative work.

                        *

                        *   2. Any pre-existing intellectual property disclaimers, notices, or terms
```

```
*      and conditions. If none exist, a short notice of the following form

*      (hypertext is preferred, text is permitted) should be used within the

*      body of any redistributed or derivative code: "Copyright ©

*      [$date-of-software] World Wide Web Consortium, (Massachusetts

*      Institute of Technology, Institut National de Recherche en

*      Informatique et en Automatique, Keio University). All Rights

*      Reserved. http://www.w3.org/Consortium/Legal/"

*

*   3. Notice of any changes or modifications to the W3C files, including the

*      date changes were made. (We recommend you provide URIs to the location

*      from which the code is derived.)

*

* THIS SOFTWARE AND DOCUMENTATION IS PROVIDED "AS IS," AND COPYRIGHT HOLDERS

* MAKE NO REPRESENTATIONS OR WARRANTIES, EXPRESS OR IMPLIED, INCLUDING BUT

* NOT LIMITED TO, WARRANTIES OF MERCHANTABILITY OR FITNESS FOR ANY PARTICULAR

* PURPOSE OR THAT THE USE OF THE SOFTWARE OR DOCUMENTATION WILL NOT INFRINGE

* ANY THIRD PARTY PATENTS, COPYRIGHTS, TRADEMARKS OR OTHER RIGHTS.

*

* COPYRIGHT HOLDERS WILL NOT BE LIABLE FOR ANY DIRECT, INDIRECT, SPECIAL OR

* CONSEQUENTIAL DAMAGES ARISING OUT OF ANY USE OF THE SOFTWARE OR

* DOCUMENTATION.

*

* The name and trademarks of copyright holders may NOT be used in advertising

* or publicity pertaining to the software without specific, written prior

* permission. Title to copyright in this software and any associated

* documentation will at all times remain with copyright holders.

*
```

ZLIB LICENSE

* zlib.h -- interface of the 'zlib' general purpose compression library
  version 1.2.3, July 18th, 2005

Copyright (C) 1995-2005 Jean-loup Gailly and Mark Adler

This software is provided 'as-is', without any express or implied
  warranty. In no event will the authors be held liable for any damages
  arising from the use of this software.

  Permission is granted to anyone to use this software for any purpose,
  including commercial applications, and to alter it and redistribute it
  freely, subject to the following restrictions:

  1. The origin of this software must not be misrepresented; you must not
     claim that you wrote the original software. If you use this software
     in a product, an acknowledgment in the product documentation would be
     appreciated but is not required.
  2. Altered source versions must be plainly marked as such, and must not be
     misrepresented as being the original software.
  3. This notice may not be removed or altered from any source distribution.

  Jean-loup Gailly jloup@gzip.org
  Mark Adler madler@alumni.caltech.edu

GENERAL BSD LICENSE

Copyright (c) 1998, Regents of the University of California

All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

"Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.

"Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

"Neither the name of the <ORGANIZATION> nor the names of its contributors may be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDERS AND CONTRIBUTORS "AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE COPYRIGHT OWNER OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

GENERAL MIT LICENSE

Copyright (c) 1998, Regents of the Massachusetts Institute of Technology

Permission is hereby granted, free of charge, to any person obtaining a copy of this software and associated documentation files (the "Software"), to deal in the Software without restriction, including without limitation the rights to use, copy, modify, merge, publish, distribute, sublicense, and/or sell copies of the Software, and to permit persons to whom the Software is furnished to do so, subject to the following conditions:

The above copyright notice and this permission notice shall be included in all copies or substantial portions of the Software.

THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT. IN NO EVENT SHALL THE AUTHORS OR COPYRIGHT HOLDERS BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER LIABILITY, WHETHER IN AN ACTION OF CONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF OR IN CONNECTION WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS IN THE SOFTWARE.

UNICODE LICENSE

UNICODE, INC. LICENSE AGREEMENT - DATA FILES AND SOFTWARE

Unicode Data Files include all data files under the directories http://www.unicode.org/Public/, http://www.unicode.org/reports/, and http://www.unicode.org/cldr/data/ . Unicode Software includes any source code published in the Unicode Standard or under the directories http://www.unicode.org/Public/, http://www.unicode.org/reports/, and http://www.unicode.org/cldr/data/.

NOTICE TO USER: Carefully read the following legal agreement. BY DOWNLOADING, INSTALLING, COPYING OR OTHERWISE USING UNICODE INC.'S DATA FILES ("DATA FILES"), AND/OR SOFTWARE ("SOFTWARE"), YOU UNEQUIVOCALLY ACCEPT, AND AGREE TO BE BOUND BY, ALL OF THE TERMS AND CONDITIONS OF THIS AGREEMENT. IF YOU DO NOT AGREE, DO NOT DOWNLOAD, INSTALL, COPY, DISTRIBUTE OR USE THE DATA FILES OR SOFTWARE.

COPYRIGHT AND PERMISSION NOTICE

Copyright © 1991-2006 Unicode, Inc. All rights reserved. Distributed under the Terms of Use in http://www.unicode.org/copyright.html.

Permission is hereby granted, free of charge, to any person obtaining a copy of the Unicode data files and any associated documentation (the "Data Files") or Unicode software and any associated documentation (the "Software") to deal in the Data Files or Software without restriction, including without limitation the rights to use, copy, modify, merge, publish, distribute, and/or sell copies of the Data Files or Software, and to permit persons to whom the Data Files or Software are furnished to do so, provided that (a) the above copyright notice(s) and this permission notice appear with all copies of the Data Files or Software, (b) both the above copyright notice(s) and this permission notice appear in associated documentation, and (c) there is clear notice in each modified Data File or in the Software as well as in

the documentation associated with the Data File(s) or Software that the data or software has been modified.

THE DATA FILES AND SOFTWARE ARE PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OF THIRD PARTY RIGHTS. IN NO EVENT SHALL THE COPYRIGHT HOLDER OR HOLDERS INCLUDED IN THIS NOTICE BE LIABLE FOR ANY CLAIM, OR ANY SPECIAL INDIRECT OR CONSEQUENTIAL DAMAGES, OR ANY DAMAGES WHATSOEVER RESULTING FROM LOSS OF USE, DATA OR PROFITS, WHETHER IN AN ACTION OF CONTRACT, NEGLIGENCE OR OTHER TORTIOUS ACTION, ARISING OUT OF OR IN CONNECTION WITH THE USE OR PERFORMANCE OF THE DATA FILES OR SOFTWARE.

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

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

MISCELLANEOUS ATTRIBUTIONS

Adobe, Acrobat, and the Acrobat Logo are registered trademarks of Adobe Systems Incorporated.

FAST Instream is a trademark of Fast Search and Transfer ASA.

HP-UX is a registered trademark of Hewlett-Packard Company.

IBM, Informix, and DB2 are registered trademarks of IBM Corporation.

Jaws PDF Library is a registered trademark of Global Graphics Software Ltd.

Kofax is a registered trademark, and Ascent and Ascent Capture are trademarks of Kofax Image Products.

Linux is a registered trademark of Linus Torvalds.

Mac is a registered trademark, and Safari is a trademark of Apple Computer, Inc.

Microsoft, Windows, and Internet Explorer are registered trademarks of Microsoft Corporation.

MrSID is property of LizardTech, Inc. It is protected by U.S. Patent No. 5,710,835. Foreign Patents Pending.

Oracle is a registered trademark of Oracle Corporation.

Portions Copyright © 1994-1997 LEAD Technologies, Inc. All rights reserved.

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

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

Portions Copyright © 1997 Soft Horizons. All rights reserved.

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

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

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

Sybase is a registered trademark of Sybase, Inc.

UNIX is a registered trademark of The Open Group.

Verity is a registered trademark of Autonomy Corporation plc