Gimmal
Information Management for Everyone®

Contract Management

Installation and Maintenance Guide

Software Version 6.9.1

May 2016

Title: *Gimmal Contract Management Installation and Maintenance Guide V6.9.1*

Software Revision History

Publication Date	Description
October 2015	Updated to Gimmal branding.
December 2015	Updated for version 6.8.6 release.
March 2016	Updated for version 6.9 release.
May 2016	Updated for version 6.9.1 release.

If you have questions or comments about this publication, you can email TechnicalPublications@Gimmal.com. Be sure to identify the guide, version number, section, and page number to which you are referring. Your comments are welcomed and appreciated.

Contents

List of Procedures

About this Guide

Designed for the client's System Administrator responsible for the support and maintenance of the installed and active Gimmal Contract document management system, this Installation and Maintenance Guide contains conceptual and technical information about maintaining the Gimmal Contract system during daily usage including:

- Environment and system requirements, including hardware, software, and Documentum and Gimmal Contract architecture
- Required client hardware and software and network infrastructure
- Installation, deployment, configuration and configuration maintenance
- Gimmal Contract software upgrade and patch deployment and maintenance
- Scheduling jobs
- Security implementation, including the security model, users, roles, groups, scanning, document types and attributes
- Diagnostics and support

Designed to be both a learning guide and a procedure reference, this guide includes extensive blue cross-references with page numbers throughout to quickly direct the system administrator to the information needed. Cross-references are also listed in the Index. In electronic form, click a blue cross-reference to jump to that reference.

To quickly find needed content, choose from the:

- Master **Table of Contents** on page 3: **Subjects** in chapters in page number order.
- Chapter **Table of Contents**: Additionally, each chapter also begins with its own Table of Contents.
- **List of Procedures** on page 5: **procedures** in alphabetical order by the procedure's verb, such as add, edit, view.
- **Index** on page 93: **Subjects** such as Gimmal Jobs, LDAP, Permission Sets, etc., in alphabetical order

This guide also often references Documentum resources such as web sites and documents instead of repeating their content, and therefore this guide does not contain highly detailed procedures.

Understanding this guide is much easier if the System Administrator is also trained in Documentum system administration.

Examples and Conventions

The representative examples of the various Documentum and Gimmal Contract interfaces and windows in this Guide are generic and are not intended to match any organization's specific configuration of document cabinets, types, properties, or content in Gimmal Contract and Documentum.

A red asterisk * indicates that field's information is required and must be entered.

Key interface words, such as tab and field names, are indicated with these fonts:
Click the **Reference** tab.
Use the drag and drop plug-in.

Bold: Gives a word increased emphasis or indicates a button or other element on the interface.

Italics: Highlights a word as having a specific Gimmal Contract meaning.

Blue: Indicates a cross-reference to additional supportive or related information, such as:
See "Auto File Documents" on page 111.

More detail: Presents additional detail about the current task, usually more details about requirements and exceptions. Read these details for a fuller understanding of the task or to learn a shortcut.

ALERT! Indicates that taking this action **cannot** be undone or restored and helps the user avoid taking an incorrect action.

Environment and System Requirements

This chapter includes the following topics:

Overview of Requirements

Gimmal Contract Management extends the Documentum Web Development Kit (WDK) application environment. The Documentum Content Server and WDK application environment must be installed before installing Gimmal Contract Management.

For complete WDK details, see EMC Documentum's *Web Development Kit Release Notes*, Version 6.7, SP2 P24.

The environment and system requirements for Gimmal Contract Management include:

- Physical environment (Hardware)
- Browser environment
- Application server environment
- Software requirements
- Software requirements
- Additional operating environments
- Associated software

Gimmal Contract Management installed on premise is supported by a wide range of hardware and software. For details, see the separate *Gimmal Contract Management On Premise Supported Environments Apr_2014*.

Gimmal Contract Management Physical Environment

See Figure 1-1 for an example of the Gimmal Contract Management physical environment.

Figure 1-1 Gimmal Contract Management Physical Environment

Metadata stored in RDBMS (Oracle, SQL Server, DB2)

User Interface delivered by web application server (Tomcat, Weblogic, Websphere)

Documentum Content Server provides content repository functionality.

Content stored in file system (local, SAN, NAS or CAS).

Global users access via Web browser.
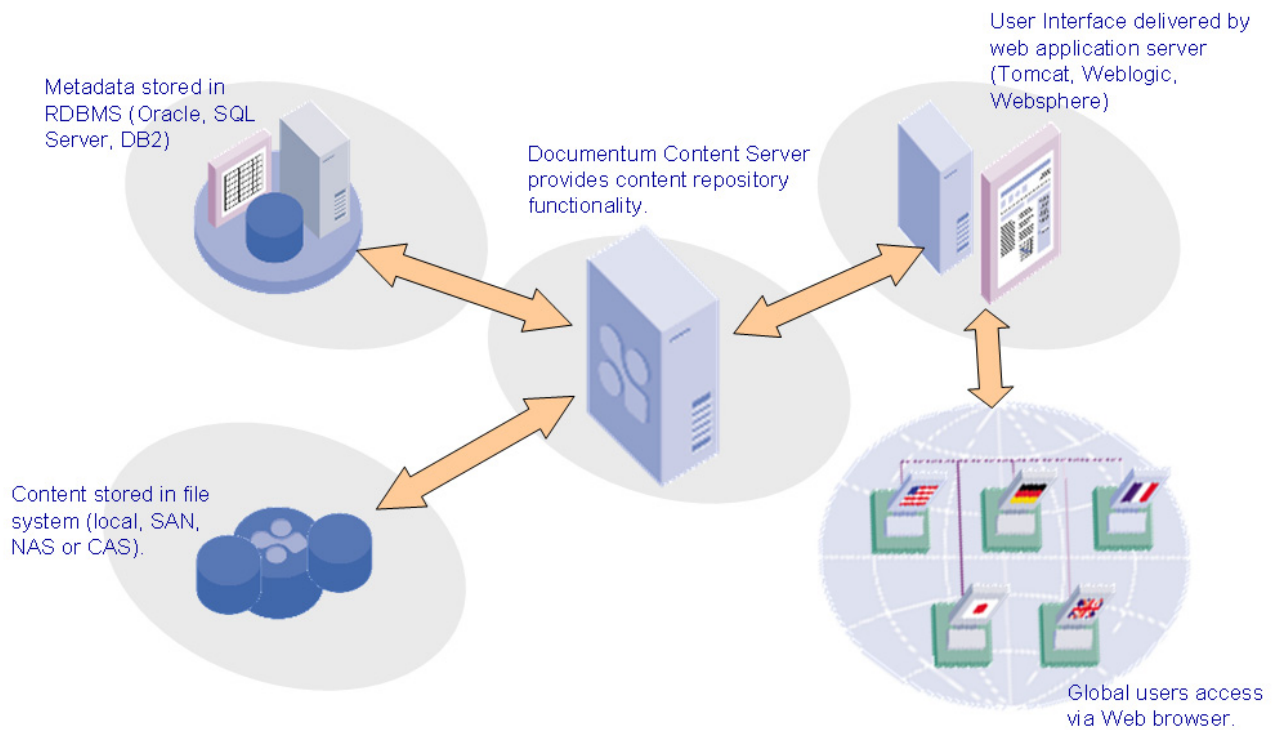
Gimmal Contract Management and Documentum Content Management System

See Figure 1-2 for an example of a Gimmal Contract Management and Documentum Content Management system.

Figure 1-2   Gimmal Contract Management and Documentum Content Management System

Prod Contract and Documentum 6
Content Management System
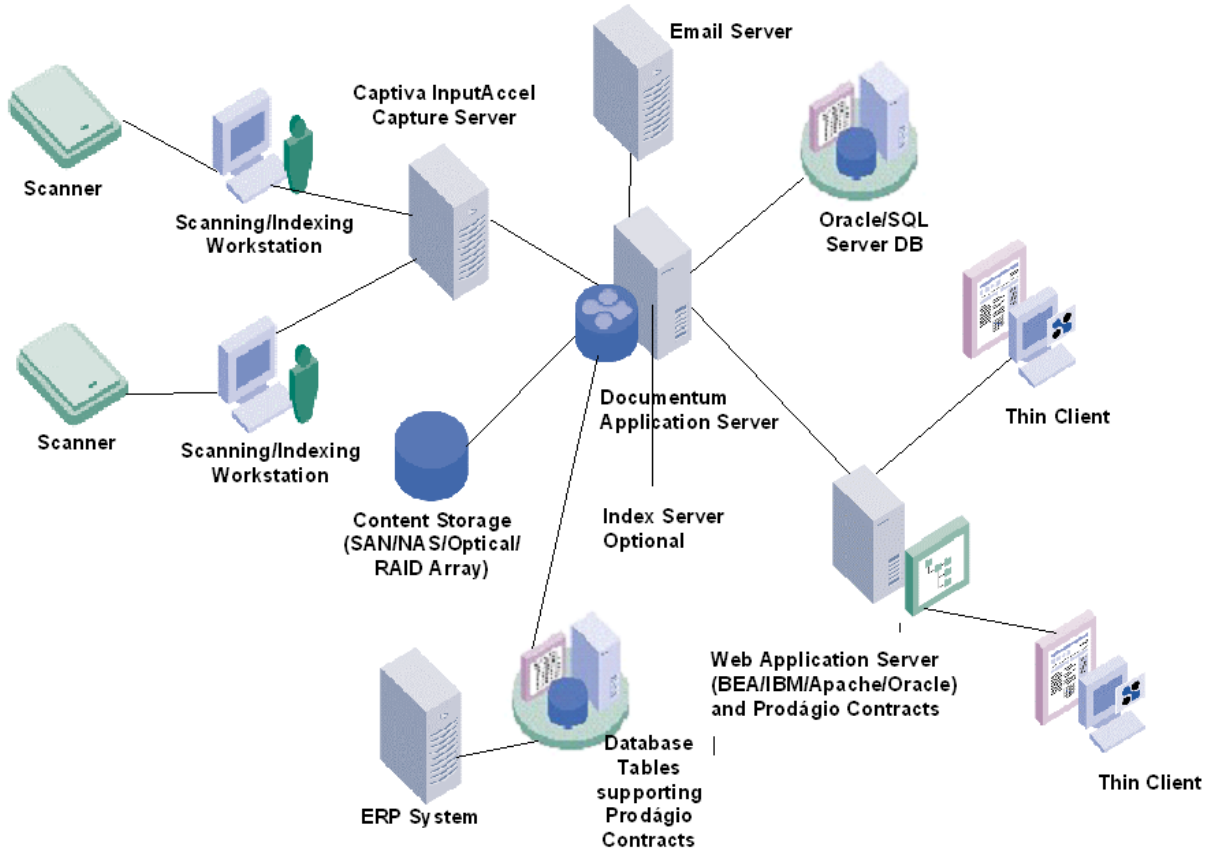
Hardware

Individual hardware requirements vary depending on factors such as the software application installed, size of deployment, number of users, and network latency. The *Documentum System Sizing Guide* provides an in-depth analysis of system sizing requirements for implementation and deployment of Documentum systems and dynamically generates estimates of hardware resource requirements based on user and hardware profiles.

Download the Documentum System Sizing Tool from the EMC Developer Network web site **http:eveloper.emc.com/developer** and click **DCTMSystemSizingTool.zip**.

Several considerations must be taken into account to specify Documentum environment hardware requirements. Among these are:

- The number of end users and the number of concurrent end users
- The volume of documents being processed
- Performance and speed requirements
- Workflow requirements
- System availability requirements (capacity)
- Adequacy of existing network infrastructure
- Centralized or distributed processing

Table 1 presents sample hardware recommendations for Microsoft products.

Table 1   Sample Hardware Recommendations (Microsoft)

Documentum Content Server (Application Server) Version 7.2	**Windows Server 2008 R2 or Windows Server 2012 R2 (2) 2.8 GHz CPUs 8GB RAM 80GB RAID5 Disk Array**
Documentum Content Store	**NAS capable of being an I-SCSI target**
Database Server	**Windows Server 2008 R2 or Windows Server 2012 R2 (4) 2.8 GHz CPUs 8GB RAM 100 GB RAID5 Disk Array**
Web Application Server	**Windows Server 2008 R2 or Windows Server 2012 R2 (2) 2.8 GHz CPUs 4GB RAM 80 GB RAID5 Disk Array**

Index Server	**Windows Server 2008 R2 or** **Windows Server 2012 R2** **(2) 2.8 GHz CPUs** **8GB RAM** **100 GB RAID5 Disk Array**
Application Installer Workstation	**Windows 7 or Windows 8.1** **2.0+ GHz CPU** **4GB AM** **100GB Drive**

Browser Environments

For Gimmal Contract Management, the client device must be able to run the supported browser configurations, plus provide whatever disk space, RAM, or CPU requirements that might be specified by Gimmal Contract Management.

The user interface for Gimmal Contract Management runs in a browser environment that consists of a specific combination of operating system, browser, and Java Runtime Environment (JRE).

Gimmal Contract Management might install applets and a JRE on the browser client machine. These installations require approximately 25 MB of free hard disk space and sufficient free disk space to handle checked-out and cached documents.

Gimmal Contract Management is compatible with the following browsers: Internet Explorer 10 and 11, all recent versions of Mozilla Firefox, and recent versions of Safari. For a listing of all current supported browser versions, consult current *Documentum WebTop Release Notes 6.7 SP2*.

To enable Gimmal Contract Management drag and drop functionality, the browser must include installed Active X or its equivalent. See "Enabling HTTP Content Transfer for IE Version 10.0 and 11.0" on page 34.

ALERT! All browser and search engine plug-ins and popular toolbars have **not** been tested for compatibility with the Gimmal installation. Please remove any plug-in and toolbar software from individual user workstations.

For individual workstation browser settings, see "Internet Explorer Configuration Version 10.0 and 11.0" on page 33.

Server Components

Gimmal Contract Management requires a content server, a web application server, a database server, an index server (optional) and a capture server (optional). Details of each are below.

Content Server

The Content Server is the intelligence engine, handling native content Management repository services such as version Management, workflow, and automated job processing. It is ultimately responsible for processing all access to content and metadata.

The Content Server stores content in a secure and optionally encrypted directory structure. This content can reside on any file server/NAS device in a designated Content Storage Area. Data surrounding content/configurations in the repository is stored in a database (i.e., Oracle, SQL Server, DB2). The Content Application Server controls access to the repository database. Applications that run on the Content Application Server do not access the database directly; instead, they access the repository via calls to the Documentum API layer.

A single Content Server can support a large number of individual repositories. Each repository can have unique object types and security access strategies to support a line-of-business (LOB) application.

For content server specifications, see the *Documentum Content Server Fundamentals 7.2, Documentum Content Server Release Notes 7.2 Release Notes or Documentum Content Server Fundamentals 6.7 SP2* and *Documentum Content Server Release Notes 6.7 SP2.*

Web Application Server

The Web Application Server provides the server-side Java infrastructure within which the Gimmal application operates. Popular servers include Apache Tomcat, BEA WebLogic, IBM WebSphere and Oracle.

Application Server Requirements
Hard Disk Space: Must also have sufficient free disk space to handle temporary content transfer files, which can vary substantially

RAM: The amount of RAM that is available after taking into consideration all other RAM utilization requirements

CPU: Sufficient to handle the expected processing load

Web Development Kit (WDK) runs in an application server environment. The application server environment consists of a specific combination of operating system, application server and JDK.

Gimmal Contract Management is compatible with recent versions of:

- BEA WebLogic Server and BEA WebLogic Express
- Apache Tomcat
- IBM WebSphere Application Server
- Oracle

For Web Application Server specifications, see EMC's PowerLink **http:owerlink.emc.com** for a list of exact versions as listed in *Documentum's WebTop Release Notes 6.7 SP2.*

Running Web Application Services. See the Web Application Service vendor documentation for identifying required serves.

More detail: Apache Tomcat is recommended to achieve the best performance for the Gimmal Contract Management. Apache Tomcat has a small footprint and operates in a highly efficient manner. In addition, it can be readily obtained free of charge.

Database Server

The Gimmal Contract Management repository exists as a database in the Oracle, SQL server or DB2. The database stores the metadata (properties).

Index Server (Optional)

Full-text indexing enables users to search a repository for specific text found in stored documents. It also enables accelerated searches through indexed document attributes. The index server creates full-text indexes and responds to queries from the Documentum Application Server.

Capture Server (Optional)

The Capture Server is responsible for processing scanned images including OCR (optical character recognition), indexing, converting to .PDF format and ultimately exporting to the Documentum repository to enable further processing through the Gimmal Contract Management interface.

Software Requirements

For information on currently supported environments and future updates, refer to Product Information System on the PowerLink website: **http:owerlink.emc.com**. For detailed information about the policies governing supported products, refer to the ESG Customer Guide available on the PowerLink website: **http:owerlink.emc.com**.

Associated Software

Other software associated with the Gimmal Contract Management installation includes:

- Documentum Administrator (DA) – for Management of users, groups, roles and document types. See "Maintenance of Users And Roles" on page 62.
- Documentum Reporting Services (DRS) – for optional installation of Crystal Reports.
- Documentum Composer and Documentum Archive (DAR) - used to install updates. See "Installing Gimmal EBS and JAR Files" on page 28.
- Capture server software controlling the scanning process – see "Capture Server (Optional)" on page 9.

Gimmal Contract Management Installation and Maintenance Guide V6.9.1

Installing and Upgrading Gimmal Contract Management

This chapter presents the following topics:

Installing Gimmal Contract Management

This section outlines the typical steps required to install Gimmal Contract Management.

Consult the required Documentation documentation for installation details. See "Documentum Reference Documentation" on page 29.

Gimmal Contract Management Installation Procedure

1 Install Hardware / OS (if necessary).
   Review Documentum product release notes.

2 Install Database Management System (DBMS) per vendor instructions.

3 Install Content Server per vendor instructions.
   Reference: EMC Documentum Content Server Installation Guide
   To limit the number of results from a DQL query, in the server. ini file add this parameter:
   return_top_results_row_based = F

4 Create Repository per vendor instructions.
   Reference: *ContentServerInstallGuide_6.7 SP2.pdf* or later

5 Install Repository Configurations
   See "Install Gimmal Repository Configurations with DAR Deployer" on page 18.

6 Install Web Application Server per vendor instructions.

7 Install Documentum Administrator Web Application per vendor instructions.
   Reference: *Documentum Administrator Deployment Guide*

8 Install Gimmal Web Application.
   See "Web Application Installation" on page 15.

9 Install Index Server (if necessary) per vendor instructions.
   Reference: *Documentum Content Server Fulltext Indexing System Installation and Administration Guide*

10 Install Document Transformation Services (if necessary) per vendor instructions.
   Reference: Documentum Document Transformation Services Installation Guide

11 Install Document Capture Services (if necessary)
   Install per vendor instructions.

12 Install Documentum Reporting Services (if necessary)
   Install per vendor instructions.
   Reference: *Documentum Reporting Services Installation Guide*

More detail: The DRS components are already installed in the Gimmal application.

13 Install Gimmal EBS and JAR Files
   See "Installing Gimmal EBS and JAR Files" on page 28.

Web Application Installation

1 Install Gimmal Contract Management .war/.ear file per the web application server instructions.

2 Create a dfc.properties file per Documentum instructions to a network accessible location. Example:

    dfc.docbroker.host[0]=devweb01d65
    dfc.docbroker.port[0]=1489
    dfc.globalregistry.repository=Global_Repository_65
    dfc.globalregistry.username=dm_bof_registry
    dfc.globalregistry.password=GrRNPhLJrkoTDAZE0RGJow\=\=

3 Launch the Gimmal Contract Management application in a supported browser window. The login page displays. See Figure 2-1.

Figure 2-1 Login

4 Click the **Browse** button for the **DFC File**.

5 Select the dfc.properties file created in step 2; then click **Open**.

6 The login page refreshes with the Repository list from the configured Docbroker(s). See Figure 2-2.

More detail: It might be necessary to restart the web server after this process.

Figure 2-2   Login Window with Repository

7 After login, the dfc.properties file can be updated through the Gimmal administration
   component.

Upgrading Gimmal Contract Management

This section outlines the typical steps required to upgrade and existing Gimmal Contract Management installation.

Before beginning any Gimmal Contract Management upgrade:

1. Run full system backups.

2. Run the upgrade process on the development environment first.

3. Perform the upgrade after all sessions have been disconnected.

These upgrade instructions assume that:

- The latest version of the Documentum Content Server has been installed. Please refer to *Documentum Content Server Installation Guide.*
- All Gimmal Content Server Docbases have been upgraded.

When installing Gimmal Contract Management releases, stop and restart the Web Application Server for any updates to take effect. If the Web Application Server runs as a service, then stop and restart the service. Alternatively, if the Web Application Server executes at the command line, issue the appropriate batch commands to stop and restart the Web Application Server.

ALERT! All Gimmal Contract Management specific folders located under the Web Application directory structure must have execute privileges for the application to operate correctly.

The Documentum and Object Model installation steps upgrades and new releases might not be needed. Web Location and Method Server installation steps **must** be performed.

Gimmal Contract Management Upgrade Procedure

1 Update Hardware / OS (if necessary) per vendor instructions.
   Review Documentum product release notes.

2 Update Database Management System (DBMS) (if necessary) per vendor instructions.
   Review Documentum product release notes.

3 Update Web Application Server (if necessary) per vendor instructions.
   Review Documentum product release notes.

4 Update Content Server per vendor instructions.
   Reference: *Documentum Content Server Installation Guide*

5 Install Documentum Composer See "Installing Documentum Composer" on page 18.

6 Update Index Server (if necessary) per vendor instructions.
   Reference: *Documentum Content Server Fulltext Indexing System Installation and Administration Guide*

7 Update Document Transformation Services (if necessary) per vendor instructions.
   Reference: *Documentum Document Transformation Services Installation Guide*

8 Update Document Capture Services (if necessary) per vendor instructions.

9 Update Documentum Reporting Services (if necessary) per vendor instructions.
Reference: *Documentum Reporting Services Installation Guide*

10 Update Documentum Administrator Web Application (ear/war file) per vendor instructions.
Reference: *Documentum Administrator Deployment Guide*

11 Update Gimmal Configurations
See "Install Gimmal Repository Configurations with DAR Deployer" on page 18.

12 Update Gimmal Web Application.
See "Installing Updated Gimmal Web Application" on page 25.

13 Update Gimmal EBS and JAR Files
See "Installing Gimmal EBS and JAR Files" on page 28

Installing Documentum Composer

Composer is delivered in the form of a compressed ZIP file that contains the Eclipse platform and all required plug-ins.

Install Composer

1 Download the DCTM_Composer_R.6.7_SP2_Patch21.zip file from the download site (http:owerlink.EMC.com):

2 Extract the ZIP file to a directory on your local drive.

3 Configure the connection broker:

   A Change to the ...\Composer\plugins directory.

   B Double-click the com.emc.ide.external.dfc_1.00 folder.

   C Double-click the documentum.config folder.

   D Open the dfc.properties file with a text editor, such as Notepad.

   E Add the DFC and connection broker information, similar to:
   dfc.docbroker.host[0]=[DocBroker IP address or host name]

4 Save all changes.

Install Gimmal Repository Configurations with DAR Deployer

Prerequisites

1 Eclipse Composer and the Documentum Archive (DAR) installer plug-in must be installed on a windows workstation. See the Documentum documentation about downloading and installing Composer and DAR Deployer plug-in for more details.

2 Gimmal Contract Management DAR file or Gimmal Contract Management Upgrade DAR file must be saved on the local machine.

3 Documentum Content Server must be installed and the following information must be known:

- The docbroker host
- The repository name
- The repository install owner ID
- The repository install owner password

Installation Process

1 Run darinstaller.exe, which is located in the Composer root directory, to start the Documentum Archive (DAR) Installer plugin.

2 When opening the DAR Deployer program, it creates three folders in the Composer installation directory:

- darinstallerconfig – Contains configuration files for the DAR Deployer program
- darinstallerlogs – The default location of the log files
- darinstallerworkspaces - Workspaces that are created and used by the DAR Deployer program. See Figure 2-3.

Figure 2-3   DAR Deployer Folders

3 The DAR Deployer requires completing certain values indicated by an asterisk (*). All other fields are optional. In the DAR Details section, specify values for the fields. See Table 2.

Table 2   DAR Deployer Fields

DAR	Yes	The absolute file path to the .dar file to install. The file path cannot contain any I18N characters or the installation will fail.
Input File	No	The absolute file path to the Install-based parameter file.
Local Folder	No	The absolute file path to localized .properties files. To make the application available in other languages, localize the project data such as labels, tabs, and descriptions.
Log File	No	The file to save the log to. If this is not specified, the file defaults to <DAR>.log.
Docbroker Host	Yes	The address of the Docbroker.
Docbroker Port	Yes	The port of the Docbroker Repository.

Repository	Yes	The name of the repository to install the DAR file. Click the **Connect** button after entering the Docbroker host and port to retrieve the available repositories.
User Name	Yes	The login name for the repository.
Password	Yes	The password for logging into the repository.
Domain	No	The domain where the repository resides.

4 Browse to locate the DAR field.

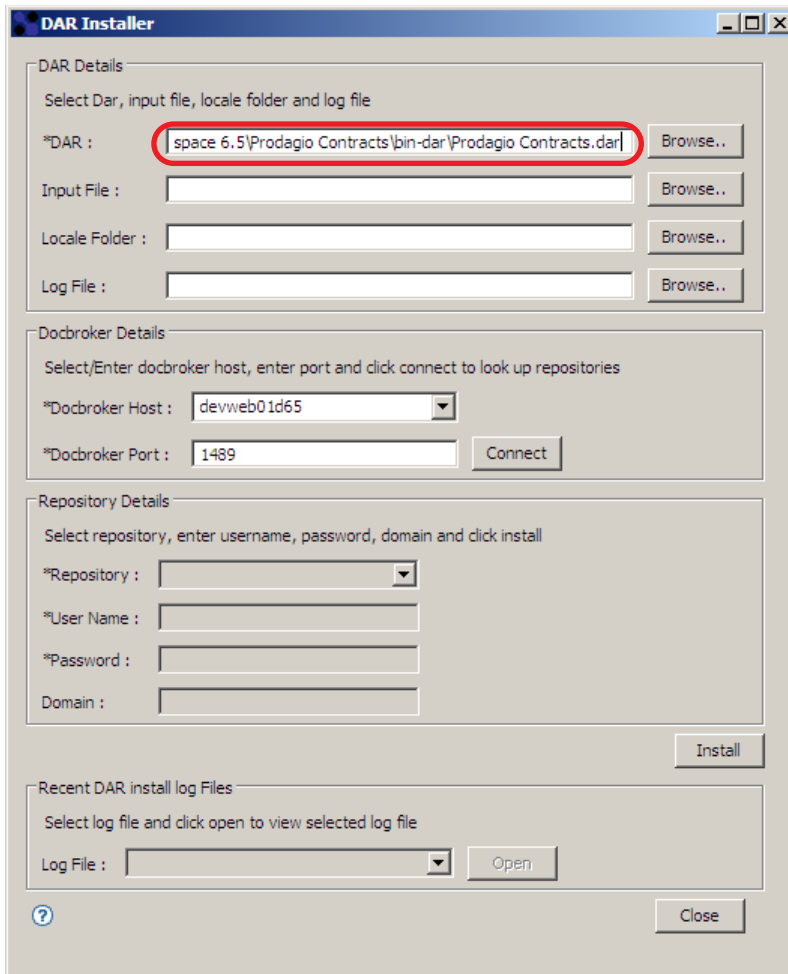A Click **Browse** next to the DAR field (Figure 2-4).

Figure 2-4   DAR Deployer
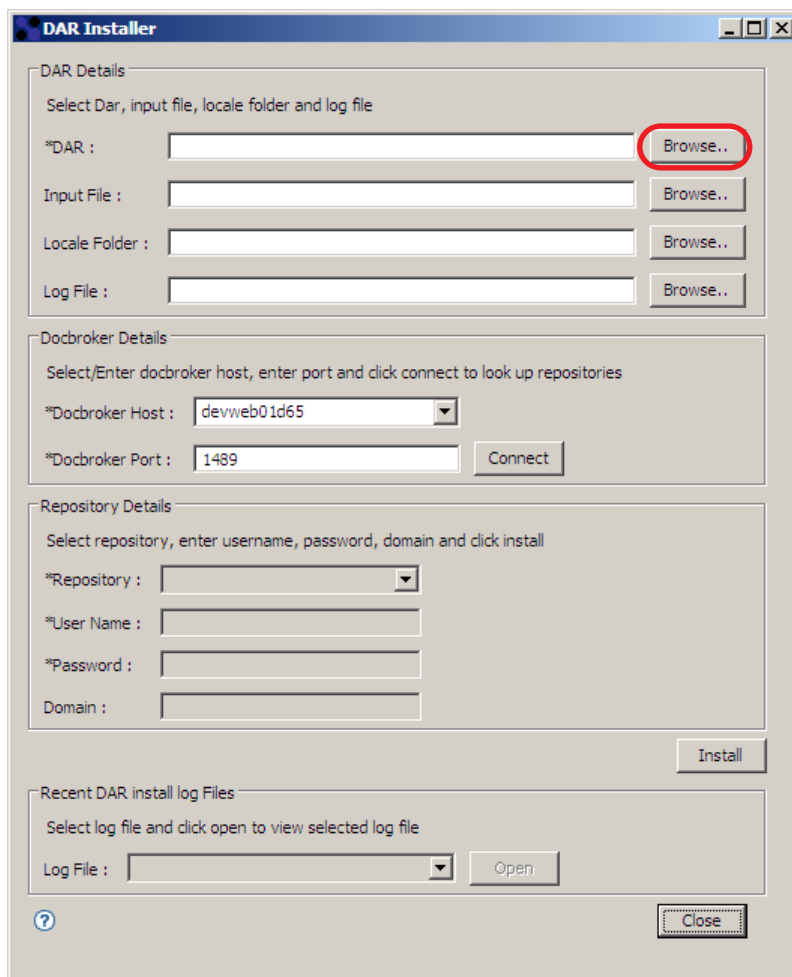
B Navigate to the folder containing the DAR file and select it. See Figure 2-5.

More detail: If this is an initial deployment, select the *Gimmal Contract Management.dar* file. If this is an upgrade, select the *Gimmal Contract Management Upgrade.dar* file.

Figure 2-5   DAR File

5 In the Docbroker Details section, specify values for Docbroker Host and Docbroker Port, and click Connect (Figure 2-6).

Figure 2-6   Docbroker Details

6 In the **Repository Details** section, specify values for **Repository**, **User Name**, and **Password**.

A Click **Install** to install the DAR file to the repository. See Figure 2-7.

Figure 2-7   Repository Details
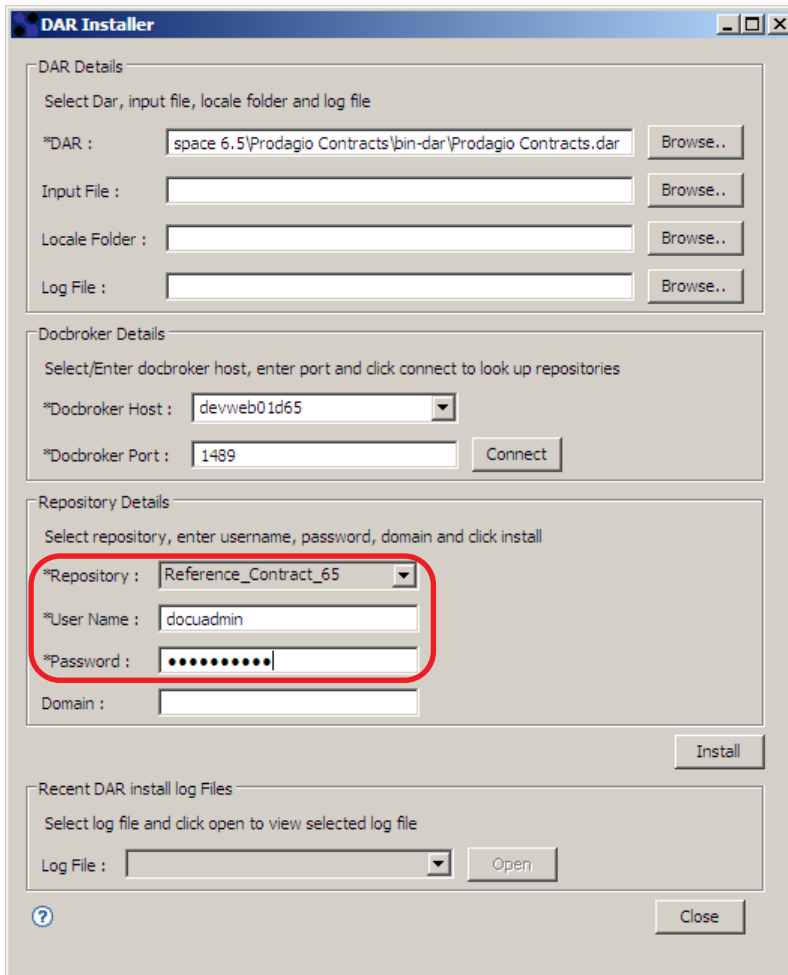
B A progress dialog displays (Figure 2-8).

Figure 2-8   Progress Dialog
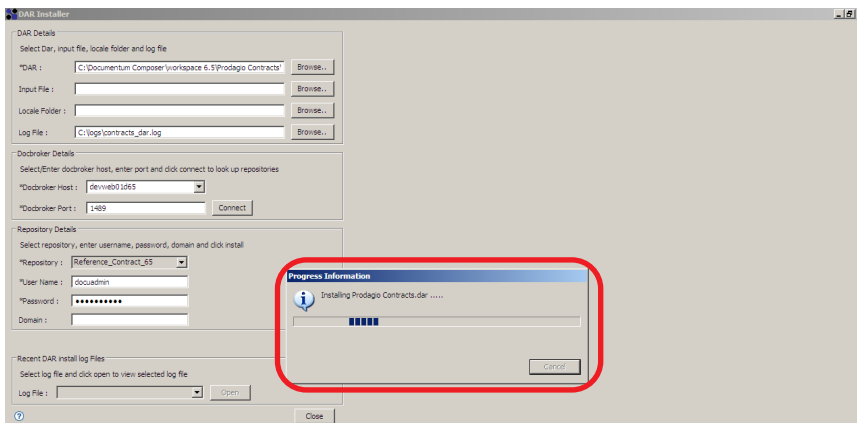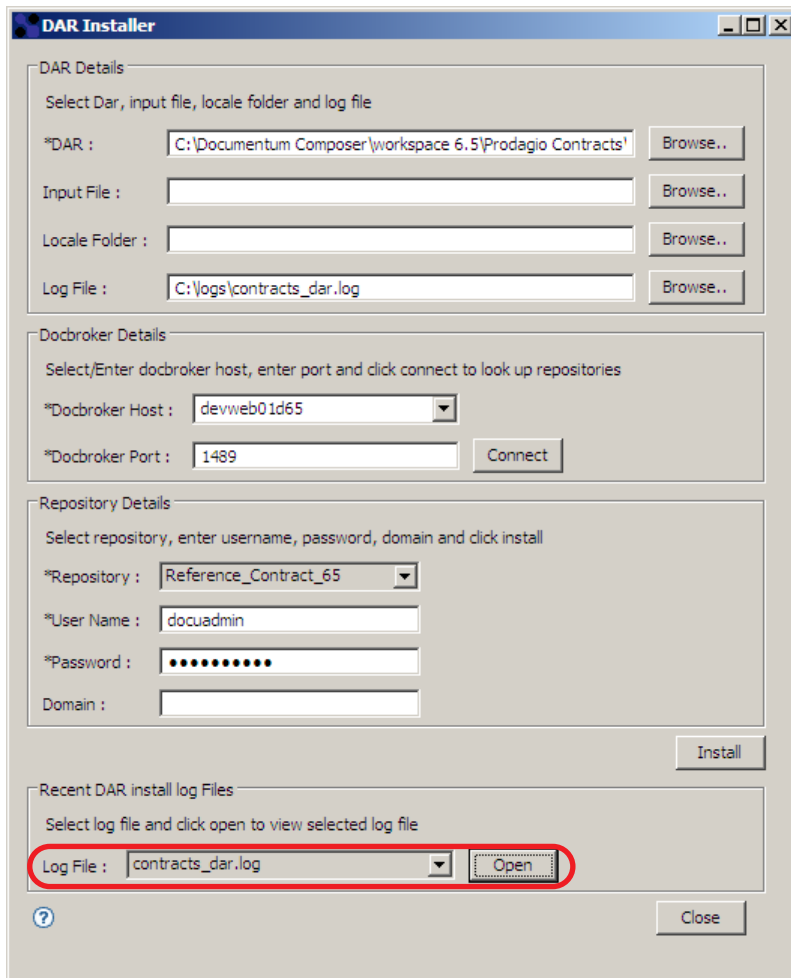
C The DAR is now installed successfully. Click **OK** and close to exit the DAR Deployer

Deployment Verification

Check the Documentum Archive (DAR) installation log for any errors.

1 To check the log for the DAR installation, select the log file from the **Log File** menu and click **Open** (Figure 2-9).

Figure 2-9   DAR Log File Location

2 Check the log file for any errors (Figure 2-9).

Figure 2-10 DAR Log File Errors
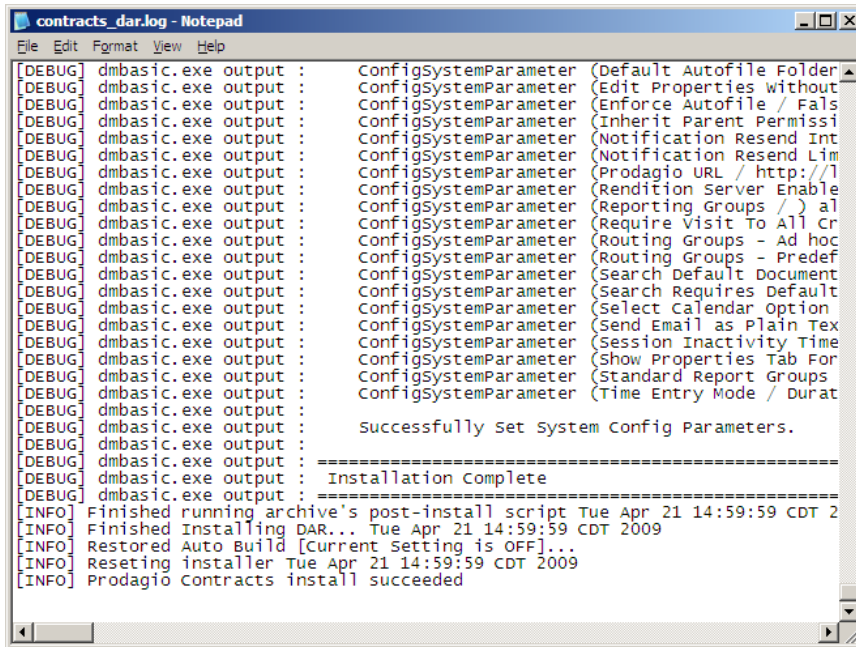
3 Contact Gimmal Support if errors display.

Workspace Cleanup

The Documentum Archive (DAR) program does not automatically delete the workspaces it creates in the darinstallerworkspaces directory. Occasionally, you must clean up this directory. The workspace directories are named in the following format:

darinstaller_workspace_yyyy-mm-dd-hh-mm-ss

See Figure 2-11.

Figure 2-11 DAR Workspace Directories

Installing Updated Gimmal Web Application

1 Uninstall the previous Gimmal Contract Management web application version.

2 Install the .war/.ear file per vendor instructions.

3 Create a dfc.properties file per Documentum instructions to a network accessible location.

Example:

dfc.docbroker.host[0]=devweb01d65

dfc.docbroker.port[0]=1489
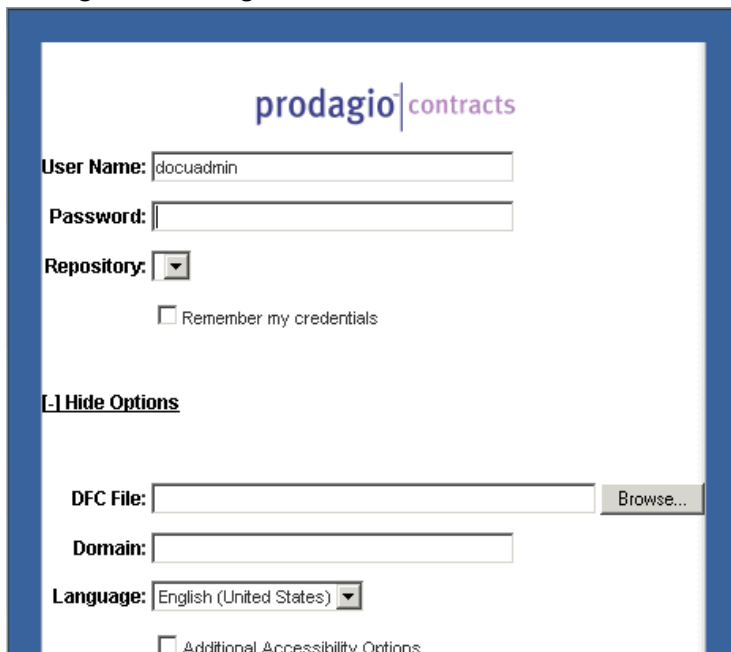
dfc.globalregistry.repository=Global_Repository_65

dfc.globalregistry.username=dm_bof_registry

dfc.globalregistry.password=GrRNPhLJrkoTDAZE0RGJow\=\=

4 Launch the Gimmal application in a supported browser window. The login page displays.(Figure 2-12).

Figure 2-12 Log In

5 Click **[+] More Options**

6 Click the **Browse** button for the **DFC File** field. (Figure 2-13).

Figure 2-13 Choose File
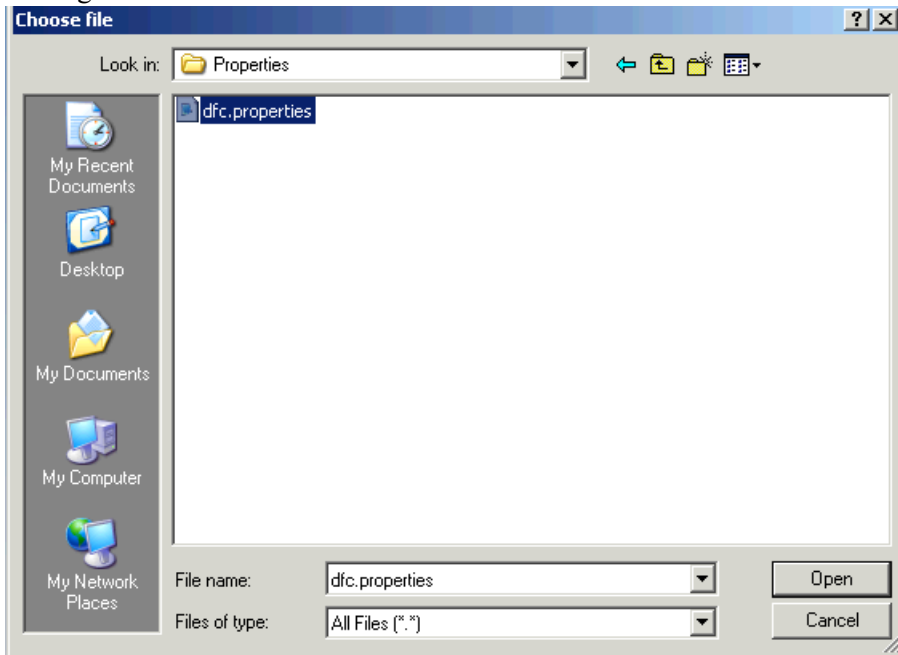
7 Select the dfc.properties file created in step 2; then click **Open**.

8 The login page refreshes with the Repository list from the configured Docbroker(s). See Figure 2-14.

Figure 2-14 Login Window with Repository

After login, the dfc.properties file can be updated through the Gimmal administration component.

Installing Gimmal EBS and JAR Files

Windows Installation

1 Copy the im_event_sender.ebs file to the ...\Documentum\product\6.7 SP2\bin directory on your content server.

2 Stop the Documentum Java method service in Task Manager, select java.exe, and click End Task.

3 Copy the ProdagioContractServer.jar file to the ...\Documentum\dba\java_methods directory on your content server.

4 Copy the xxxCustomCode.jar file (if one exists) to the ...\Documentum\dba\java_methods directory on your content server.

   A If there is an existing $Aspose.Words.xxx.jar$ file, delete it or disable it by changing its file extension to BAK; for example, Aspose.Words.xxx.jar.bak.

   B Copy the Aspose.Words.2.7.0.jdk15.jar from the deployment directory to the <DCTM_HOME>/java_methods directory.

5 Replace the activation.jar file in the method server deployment lib directory ...\Documentum\jboss4.2.0\server\DctmServer_MethodServer\deploy\ServerApps.ear\APP-INF\lib with the activation.jar from the workspace (...\GimmalCommon\lib\deploy).

6 Copy the mail.jar file from the workspace (...\GimmalCommon\lib\deploy) to the method server deployment lib directory ...\Documentum\jboss4.2.0\server\DctmServer_MethodServer\deploy\ServerApps.ear\APP-INF\lib

7 Start the Documentum Java method service.

Unix Installation

1 Copy the im_event_sender.ebs file to the .../Documentum/product/6.7 SP2/bin directory on your content server.

2 Stop the Documentum Java method service.

3 Copy the ProdagioContractsServer.jar file to the .../Documentum/dba/java_methods directory on your content server.

4 Copy the xxxCustomCode.jar file (if one exists) to the /Documentum/dba/java_methods directory on your content server.

5 Replace the activation.jar file in the method server deployment lib directory .../Documentum/jboss4.2.0/server/DctmServer_MethodServer/deploy/ServerApps.ear/APP-INF/lib with the activation.jar file from the workspace (.../GimmalCommon/lib/deploy)

6 Copy the mail.jar file from the workspace (.../GimmalCommon/lib/deploy) to the method server deployment lib directory .../Documentum/jboss4.2.0/server/DctmServer_MethodServer/deploy/ServerApps.ear/APP-INF/lib

7 Start the Documentum Java method service.

Documentum Reference Documentation

- *Documentum Content Server Installation Guide*
- *Documentum Administrator Deployment Guide*
- *Documentum Content Server Fulltext Indexing System Installation and Administration Guide*
- *Documentum Document Transformation Services Installation Guide*
- *Documentum Reporting Services Installation Guide*
- *Documentum Webtop 6.7 SP2 Release Notes*

Configuration and Maintenance

This chapter presents the following topics:

Overview of Configuration

This chapter provides information about the typical maintenance and configuration actions required for Gimmal Contract Management. Included are:

- Interface configuration
- Internet Explorer and Microsoft Word
- Jobs
- Adding and managing users
- Mail server settings
- Managing security
- Recommended server settings
- Install server-side methods
- Business administrator's system connectivity

For more information about configuration, please see the separate Documentum support documentation.

Gimmal Contract Management Interface

Gimmal Contract Management utilizes Documentum's standard client interface, WebTop, built on Documentum's Web Development Kit (WDK) framework. WDK is a JSP application. Figure 3-1 is a sample view of the Gimmal Contract Management application.

Figure 3-1 Gimmal Contract Management Client Interface
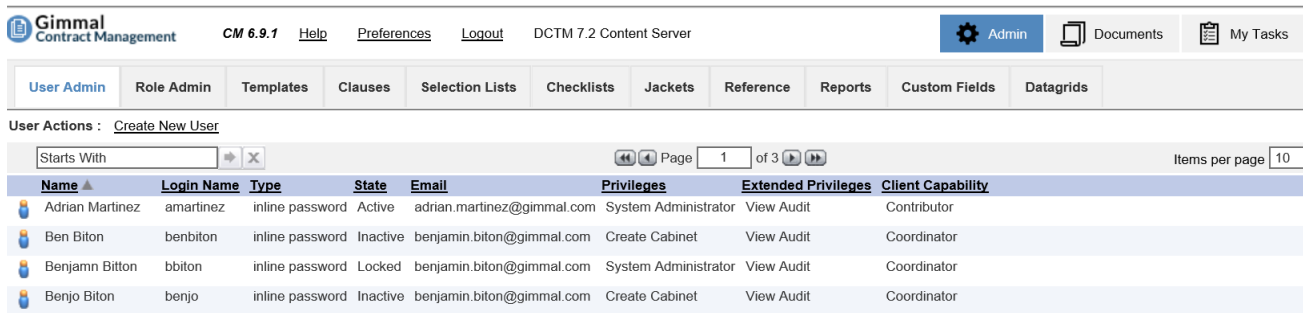
Workstation Setup

These workstation setup steps should be completed for each workstation to be used during training or before the first time any user accesses Gimmal.

Additionally, as a preventative measure, it is recommended to perform these steps on each end user workstation before starting user acceptance testing (UAT).

Workstation Sizing

Gimmal requires client workstation capable of running the supported browser configurations listed below, plus whatever disk space, RAM, or CPU requirements that might be specified by third-party products such as Microsoft Office (for editing Office-formatted documents).

A typical workstation has 4GB to 8GB RAM, a minimum 100GB Disk, and a CPU faster than 2.0 GHz.

Gimmal client applications can install applets and a JRE on the browser client workstation. This will require approximately 25 MB of free hard disk space. Additionally, sufficient free disk space is needed to handle checked out and cached documents.

Supported Browser Environments

Please consult *Documentum's Webtop 6.7 SP2 Release Notes* for any updates to the list of supported browser environments.

Internet Explorer Configuration Version 10.0 and 11.0

To ensure optimum Gimmal Contract Management operation, perform these Internet Explorer configurations at *each* Gimmal Contract Management workstation:

- "Install the Active X Plug-In"
- "Disable the Popup Blocker"
- "Configure Internet Explorer 10 and 11 Options":
  - Clear the temporary Internet files, cookies and browsing history.
  - Set Gimmal Contract Management as a Trusted website.
  - Set stored pages setting to **Every time I visit the webpage.**
  - Configure temporary Internet files to clear when Internet Explorer is closed.

Install the Active X Plug-In

To enable Gimmal Contract Management Drag and Drop functionality, install the Internet Explorer Active X plug-in on each client workstation running Internet Explorer.

More detail: Drag and Drop **cannot** be enabled if using the Firefox, Safari, or Opera browsers because these browsers do not offer an Active X component. Chrome **does** have an equivalent plug-in.

Disable the Popup Blocker

1 In the IE 10and IE 11 browsers, select **Tools**, select **Internet Options**, and click the **Privacy** tab.

2 Ensure **Turn On Pop-up Blocker** is not selected so that the popup blocker is disabled.

Configure Internet Explorer 10 and 11 Options

1 At each desktop, open Internet Explorer 10 or IE 11.

2 Click **Tools** and then **Internet Options**. The Internet Options dialog box displays its **General** tab.

Figure 3-2   General Tab in Internet Options Dialog Box
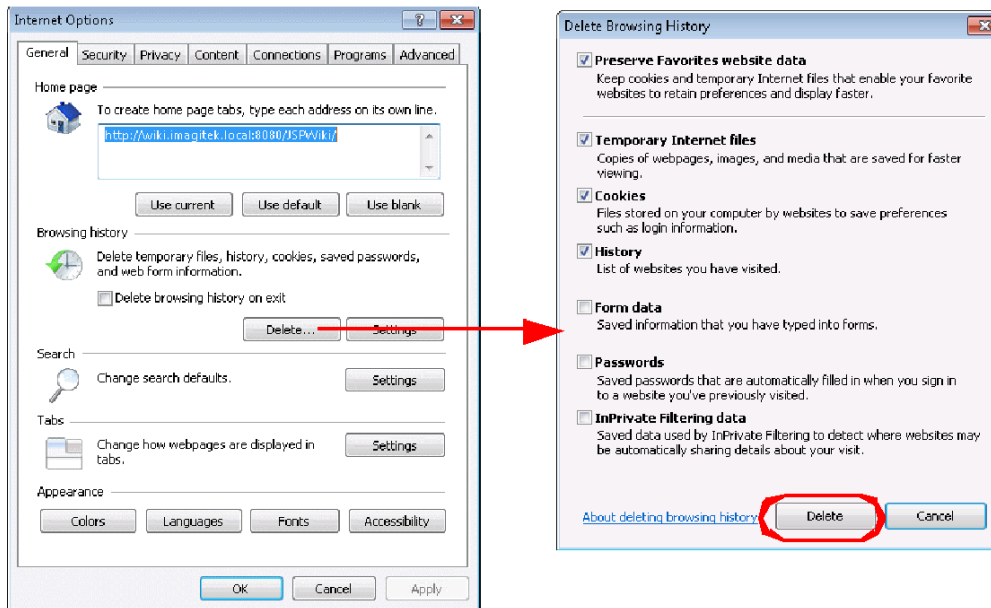
3   In the **Browsing history** section, click **Delete**. The **Delete Browsing History** window displays.

4   Select **Preserve Favorites website data**, **Temporary Internet files**, **Cookies,** and **History** to identify what to delete.

5   Click **Delete**.

6   In the **Browsing history** area, click **Settings**. The Temporary Internet Files window displays

7   Select **Every time I visit the webpage**.

8   Click **OK**.

9   On the Internet Options window, click **Settings**.

More detail: Deleting everything can free hard disk space, solve problems with your web browser, and pro-vide some additional privacy, but it might inconvenience you by removing information you might need on the Internet. For example, you will have to retype passwords that were previously stored on your computer.

Enabling HTTP Content Transfer for IE Version 10.0 and 11.0

The HTTP Content Transfer Protocol can be enabled in IE 10 and IE 11 as an alternative to using the UCF File Transfer Protocol.

Internet Explorer (IE) version 10 and 11 have a default security setting that prevents the display of the file download dialog. You must add the WDK based application URL to the list of trusted sites in the browser in order to perform checkout, view, or edit using HTTP Content Transfer.

Nothing happens when a user selects **Export to CSV** if the browser security settings are disabled for file downloads. This setting is disabled by default in IE 10 and IE 11. This setting must be enabled on each browser.

Enable HTTP Content Transfer in IE 10 and IE 11

1 In the IE 10 or IE 11 browser menu, select **Tools** and then **Internet Options** and click the **Security** tab.

2 Select **Trusted sites** and then click **Custom level**.

3 Scroll to the **Downloads** section, select **File download** and select **Enable**.

4 Click **OK** and then click **OK** again to save settings.

5 Close all browser windows and restart the browser.

Enabling HTTP Content Transfer for Firefox v37 and Greater

The HTTP Content Transfer Protocol can be enabled in Firefox as an alternative to using the UCF File Transfer Protocol.

Enable HTTP Content Transfer in Firefox Version 37

1 To open the **Options** menu in Firefox, click **Tools** and then click **Options**.

2 On the **General** tab, in the Downloads section, select **Always ask me where to save files**.

3 On the **Tabs** tab, select **Open new windows in a new tab** instead.

4 On the **Content** tab, deselect **Block pop-up windows**.

5 Click **OK** and then click **OK** again to save settings.

6 Install the Firefox add-on FireBug, which is available from mozilla.org.

System Settings (Optional)

The following are optional actions to set up the operating system on each workstation.

1 Optional: Set up a shortcut icon on the desktop to *Gimmal Contract Management*.

2 Optional: Delete the ucf folder.

   A In **Users**, double-click the **<user name>** folder.

   B Double-click the **Documentum** folder, and **delete** the **ucf** folder.

   C Close the Documentum window.

3 Optional: delete Java files.

   A Click **Start**, click **Settings**, and then click **Control Panel**.

   B Double-click **Java**. See Figure 3-3.

Figure 3-3   Java Control Panel
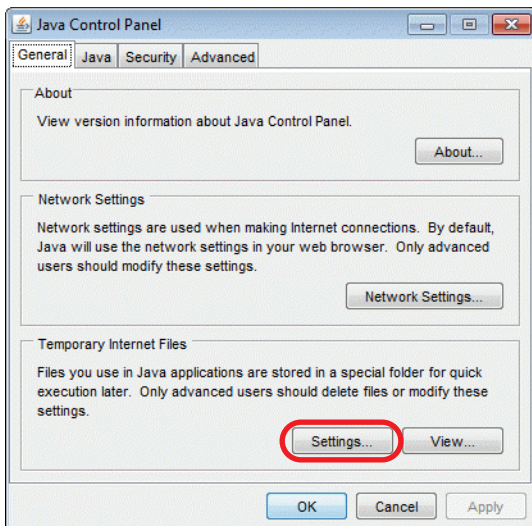
C   Click **Settings**. See Figure 3-4.

Figure 3-4   Temporary Files Settings
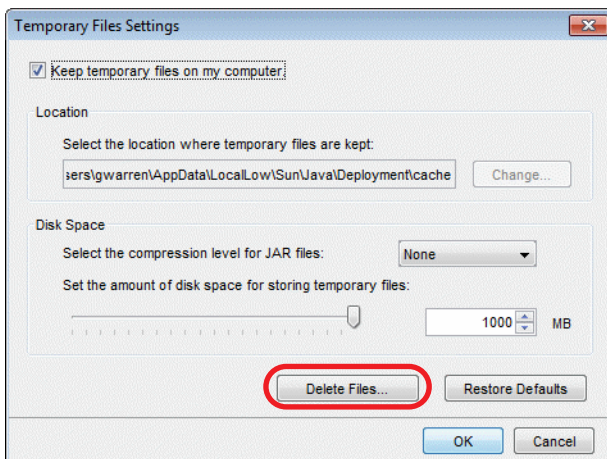
D   Click **Delete Files**.

E   Click **OK** to delete the temporary files.

F   Click **OK** to close the Temporary Files Settings window.

G   Click **OK** to close the Java Control Panel window.

H   Close the Control Panel window.

4   End any running Java processes.

A   Press **Ctrl** + **Alt** + **Delete** to display the Task Manager.

B   Click the **Task Manager** button.

C   Click the **Processes** tab (Figure 3-5).

Figure 3-5   Task Manager – Processes Tab
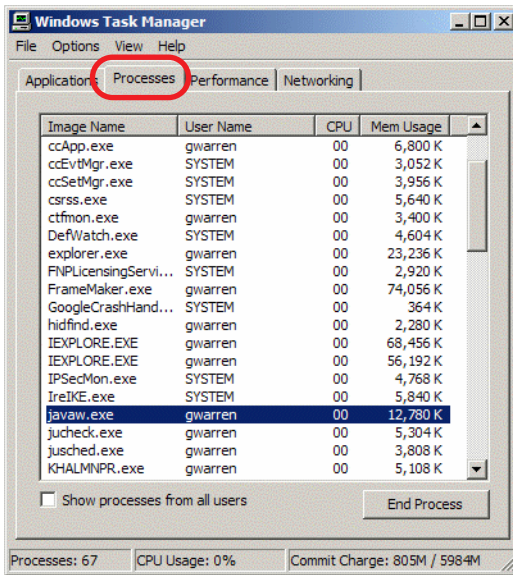
D In the **Image Name** column, select **javaw.exe** and/or **java.exe** and click **End Process**. The Task Manager Warning window displays.

E Click **Yes**.

F Close the Task Manager.

More detailed configuration settings (UCF, Java, drag and drop, add-ons, etc.) are included in the separate document *Gimmal Contract Management Desktop Troubleshooting and Configuration Guide*.

Microsoft Word Requirements

Gimmal requires Microsoft Word 2007 or later to use the Gimmal Contract Management **Creating and Applying Templates** feature.

LDAP Synchronization

Gimmal Contract Management can be synchronized to LDAP for access to directory services. See "Create a Home Cabinet for LDAP Users" on page 75.

Mail Server Setting

When a task is sent to a user's inbox (the My Tasks view), a notification can also be sent to the user's email. To enable this option, the SMTP Server property in the server configuration must be set properly. Use the Documentum Administrator to change this setting.

After changing mail server settings, restart the Web application server to enable the changed settings.

To enable the sending of email notifications from Gimmal Contract Management, the IP address of the content server must be added to the Receive Connector list on the exchange server (Figure 3-6).

Figure 3-6   SMTP Receive Connector

For more detail, see http:sexchangeteam.com/archive/2006/12/28/432013.aspx.
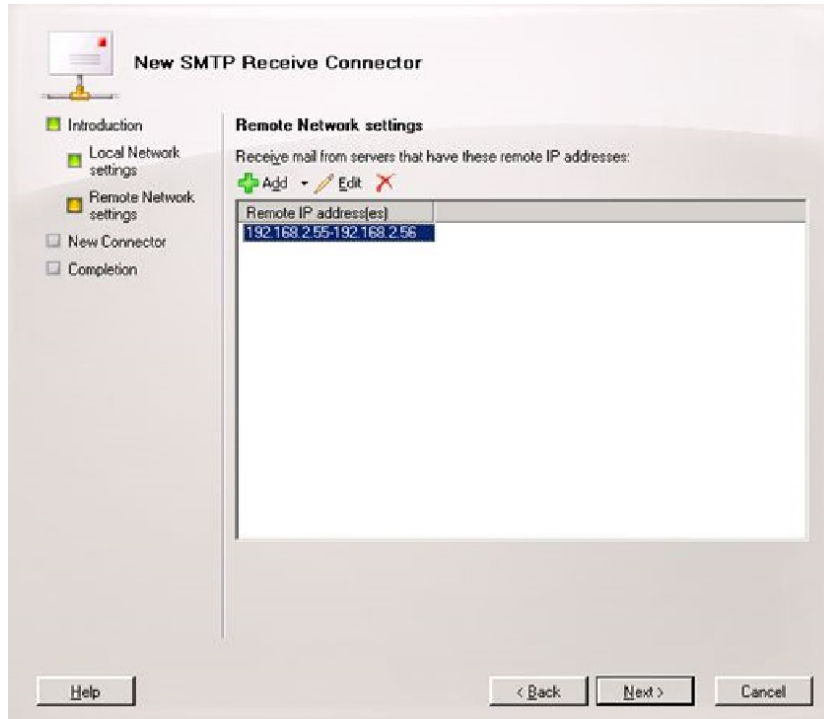
Recommended Server Settings

The following server settings are recommended for Gimmal Contract Management. These changes are made using the Documentum Administrator.

- **Repository Configuration**: Deselect the **Folder Security** option.
- **Server Configuration**: Set the property **Inherit Permission Set From** to *Type*.

More detail: A default permission set must be assigned to the **dm_sysobject** type to prevent errors when selecting this option.

After changing server settings, restart the repository services and the web server to enable the changed settings.

Disable Default Audits

In Documentum Administrator, ensure that the three default **Audit Management Names** are disabled (Figure 3-7).

Figure 3-7   Disable Default Audits
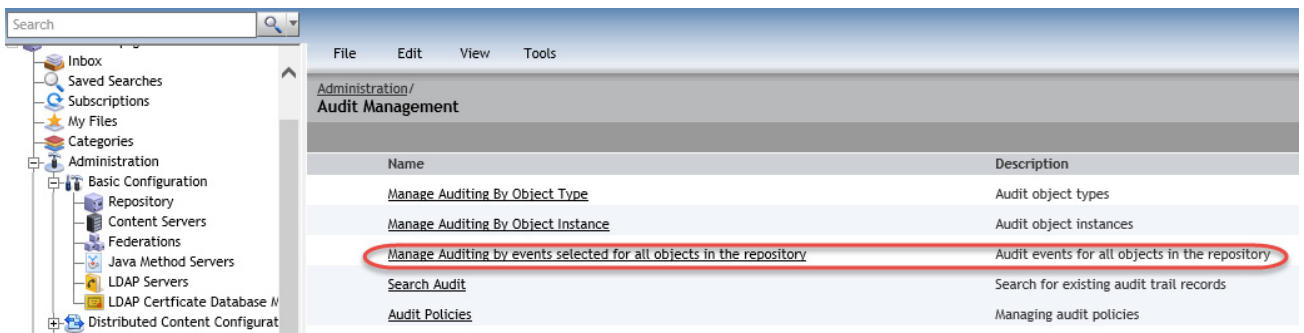
5 Click **Manage Auditing by events selected for all objects in the repository**. The following dialog box appears (Figure 3-8).

Figure 3-8   Manage Auditing Dialog Box
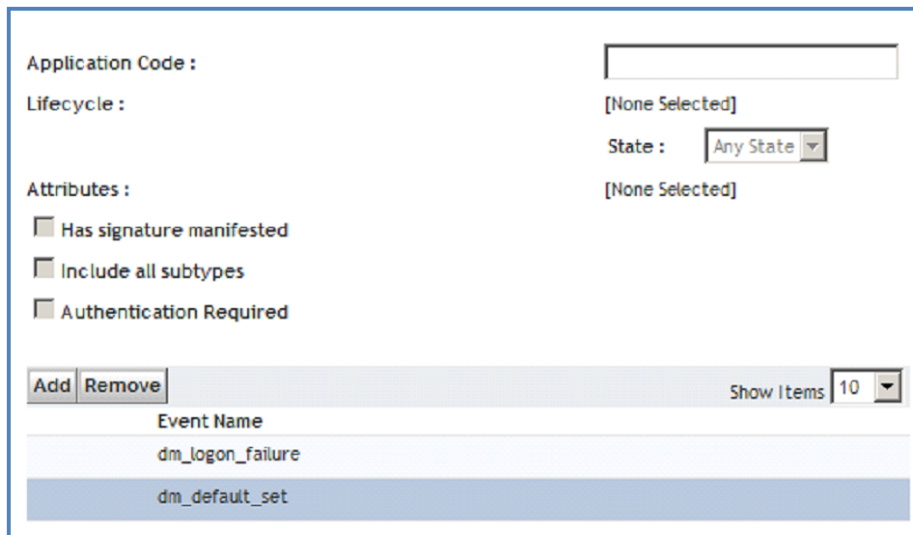
Unregister Events

If the Fast Index Server will **not** be used to index content for full-text search, unregister events for dm_fulltext_index_user.

DQL> select * from dmi_registry where user_name = 'dm_fulltext_index_user'r_object_id user_name registered_id event

2600007b80000500 dm_fulltext_index_user 0300007b80000105 dm_save

2600007b80000501 dm_fulltext_index_user 0300007b80000105 dm_destroy

2600007b80000502 dm_fulltext_index_user 0300007b80000105 dm_readonlysave

2600007b80000503 dm_fulltext_index_user 0300007b80000105 dm_checkin

2600007b80000900 dm_fulltext_index_user 0300007b80000105 dm_move_content

Then you can use the unregister API to remove these events. The syntax is

API>unregister,c,,,,

Using one of the results above, the API would look like this:

API>unregister,c,0300007b80000105,dm_save,dm_fulltext_index_user

Repeat this for each of the remaining events.

Gimmal Jobs and Methods

This chapter presents the following topics:

Gimmal Contract Jobs

The processing of notifications within Gimmal Contract is driven by automated batch jobs.

Access Gimmal Contract Jobs

1 In the left pane of the Documentum Administrator, click Administration > Job Management > Jobs.

2 In the right pane of the Documentum Administrator, select Gimmal from the menu in the upper right corner. See Figure 4-1.

Figure 4-1 Gimmal Contract Jobs
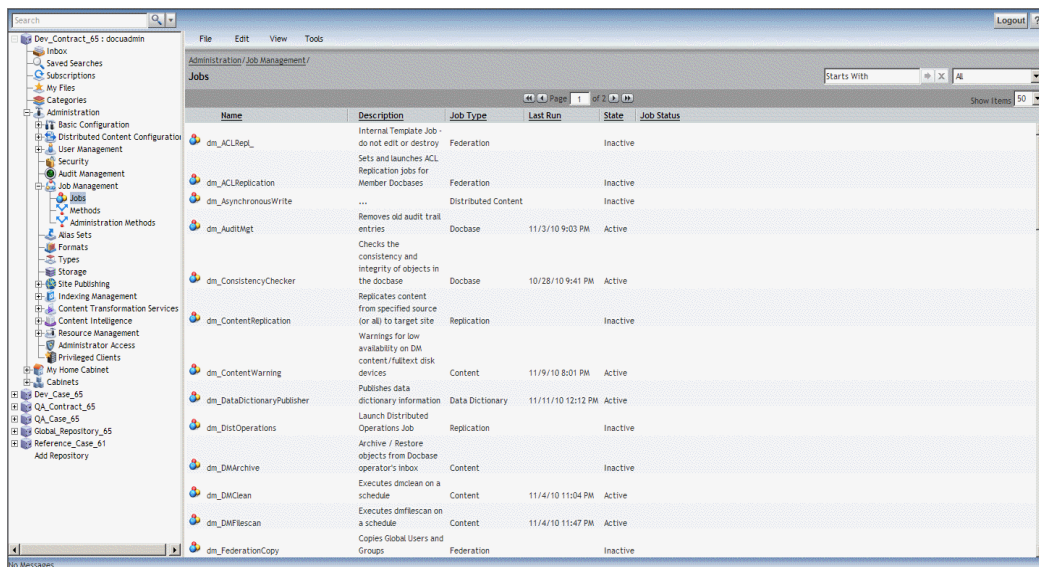
Each Product Name job has associated method content that performs the designated function. The method content for these jobs is located on the Documentum server in the <DOCUMENTUM HOME>\dba\java_methods> directory. This directory contains the GimmalContractsServer.jar file as well as any specialized client code. See Figure 4-1.

Figure 4-1 Gimmal Contract Methods
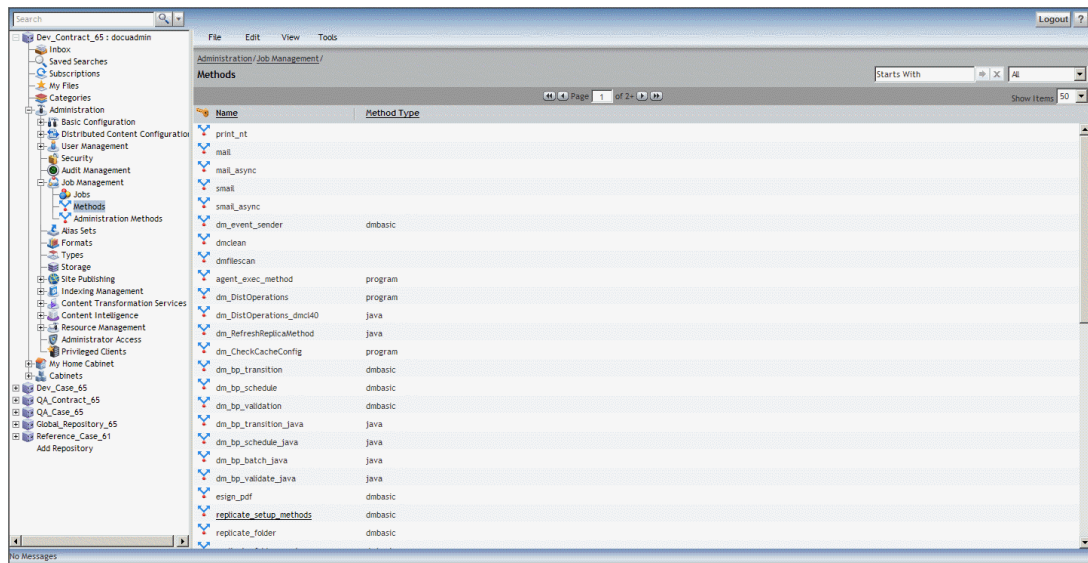
Gimmal Jobs

Jobs are scheduled to perform an activity on a regular basis. The jobs that make up the tool suite typically require very little maintenance after initially defining the execution schedules and arguments for the tools. The jobs are listed below with brief descriptions.

ALERT! It is strongly recommended to avoid changing any of these Jobs. If you feel the need to make a change, please contact Gimmal Customer Support before making any change.

IM_DocumentImportUtility

The `IM_DocumentImportUtility` job is involved with importing large amounts of document properties and documents. See "IM_DocumentImportUtility" on page 47.

IM_ExternalDataSync

The IM_ExternalDataSync job is involved with Gimmal external data synchronization. and is scheduled as business requires. See "IM_ExternalDataSync" on page 48.

IM_ExternalSelectionListSync

The IM_ExternalSelectionListSync job is involved with Gimmal external selection list synchronization and is scheduled as business requires. See "IM_ExternalSelectionListSync" on page 49.

IM_MethodDataCleanup

The IM_MethodDataCleanup job is involved with Gimmal external method data cleanup and is usually scheduled nightly. See "IM_MethodDataCleanup" on page 50.

IM_ProcessAttributes

The IM_ProcessAttributes job is involved with attribute processing and is used during diagnostics. This job is provided as a test utility for the IM_ProcessAttributes method. It will simply start, log the execution class name, and exit. This is useful in ensuring that any custom code for post-processing of object metadata is properly configured. This job should never run on a scheduled basis. See "IM_Process Attributes" on page 50.

IM_ProcessChecklists

The IM_ProcessChecklists job is involved with Gimmal Checklist item processing and is usually scheduled nightly. See "IM_ProcessChecklists" on page 50.

IM_ProcessForms

The IM_ProcessForms job is involved with Gimmal Forms data input and is scheduled as business requires. See "IM_ProcessForms" on page 51.

IM_ProcessObligations

The im_ProcessObligations job is involved with Obligation processing and is usually scheduled nightly. See .

IM_ProcessTicklers

The im_ProcessTicklers job in involved with Reminders processing and is usually scheduled nightly. See .

IM_ScheduleDateReminders

The IM_ScheduleDateReminders job is involved with Gimmal date-based Reminder processing. This job runs on a nightly basis to process any changes to the system-wide reminder rules. This will scan for all objects matching a rule that was recently modified and either generate or modify reminders for those objects in accordance with the business-defined rules. Reminders generated by this job can then be processed by IM_ProcessTicklers. See .

IM_VersionInfo

The IM_VersionInfo job is involved with Gimmal server versions and is used during diagnostics. This job is provided as an informational utility for Gimmal support. This job simply collects the output from its method in its log file. Output from this job may be requested by Gimmal Technical support in order to diagnose issues and determine the availability of fix packs or upgrades to your server side code. This job is generally not scheduled to run on a regular basis. See .

Gimmal Server Side Methods

Following is a listing of all server side methods with a brief description of its purpose and of its arguments.

IM_ApplyPermissions

The IM_ApplyPermissions method is involved with Gimmal custom permissions processing. This method is a hook point for client specific implementation of specialized permissions sets. If the Corporate Rules option is selected in the Auto File configuration, this method will be invoked when a matching Auto File operation is carried out.

Arguments: docbase – the repository on which to perform the operation
installOwner – the repository installation owner id, used to carry out the operation
objectId – the object ID on which to perform the operation
Debug – a basic flag indicating whether basic debugging is enabled

IM_ApplySignature

The IM_ApplySignature method is involved with Gimmal signature image insertion. This method is provided such that client workflows can invoke the Gimmal code to insert a signature image.

Arguments: objectId (required) – the object ID for the document to be signed
signatureType (optional) – the object type to search for the signature. This will default to im_legal_clause.
signatureLabel (strongly recommended) – the specific signature in the document to be processed. This may be omitted **only** if there is only a single signature in the document; otherwise behavior of this method is not guaranteed.
currentUser (optional) – the user who is invoking the operation
signatureId (optional) – the Documentum ID for the object containing the signature image. If omitted, either signatureCriteria must be specified OR the signatureImage tag must include the [Query Criteria] option
signatureCriteria (optional) – the criteria that are needed to locate the signature image. This is trumped by the signatureId parameter. Syntax is the same as for [Query Criteria] on the image merge field.

IM_ClearInboxTasks

The IM_CleanInboxTasks method is involved with Gimmal inbox task removal. This method clears inbox tasks (dmi_queue_item objects) that were generated for a specific Checklist, Reminder, or Obligation when that object is closed/completed. This helps users to only see those tasks that still remain to be completed rather than having to browse tasks that may have been completed by other users.

Arguments: docbase – the repository on which to perform the operation
installOwner – the repository installation owner id, used to carry out the operation
objectId – the object ID for the Checklist, Reminder, or Obligation completed/closed by the user
currentUser – the user invoking the method
event – string indicating what type of object was completed of Checklist, Obligation, or Reminder
Debug – a basic flag indicating whether basic debugging is enabled

IM_DocumentImportUtility

The `IM_DocumentImportUtility` method is involved with importing large amounts of document properties and documents. The input file MUST end with a .txt extension, even if the fields are comma separated values (csv).

Arguments

- **documentType** (required) – The document type for the import job

- **sourceDirectory** (required) – The interface directory that contains the files to be imported. Files dropped into this folder will be read, processed, and moved. **Do not use this directory for any other purpose**.

- **sourceFilePrefix** (required) – The prefix of the file to be loaded from the sourceDirectory

- **senderEmail** (optional) – An email address that the job report should come from. If not specified, the default value is the Documentum Installation Owner.

- **uniquePropertyKey** (optional) – If specified, this field is used to determine if the data should be updated or create a new record

- **autoName** (optional) – If set to True, invoke the AutoName rule for the document type to name the document. Default value is False.

- **autoFile** (optional) - If set to True, invoke the AutoFile rule for the document type to file the document. Default value is False.

- **postProcess** (optional) - If set to True, invoke the Post Processing logic when the record is imported. Default value is False.

- **notificationEmail** (optional) – If this argument is specified, an email is sent after the job completes indicating SUCCESS or ERROR. Separate multiple email addresses with a semicolon.

- **fieldDelimeter** (optional) – Specifies how the field values are delimited in the input file. Possible values are Comma, Tab and Pipe. Default value is Tab.

- **repeatDelimeter** (optional) – Specifies how fields with repeating values are delimited in the input file. Possible values are Comma, Tab and Pipe. Default value is Pipe. NOTE: **fieldDelimeter** and **repeatDelimeter** must be set to different values.

- **contentDirectory** (optional) – The directory that contains the document files to be imported. If specified, a column named **content_file** must be present in the file specified by the **sourceDirectory** argument.

Example arguments:

- documentType sales_agreement

- autoName true

- autoFile true

- postProcess true

- uniquePropertyKey document_number

- notificationEmail admin@myDomain.com; admin2@myDomain.com

- fieldDelimeter comma

- sourceDirectory \\datagateway\salesdemo

- contentDirectory \\datagateway\salesdemo

- sourceFilePrefix salesAgreement

IM_ExternalDataSync

The IM_ExternalDataSync method is involved with Gimmal external data synchronization. If Gimmal is to be synchronized with data from another master or source system, this method will be configured to read data files from a specific directory and update Gimmal with data from that file. See "IM_ExternalDataSync" on page 45.

Arguments: administratorEmail – this is the email address which will receive error notifications inputDirectory – this is the directory that will contain data files from the source system. Files dropped into this folder will be read, processed, and then deleted. **Do not use this directory for any other purpose or use an existing directory with required files.**
Debug – a basic flag indicating whether basic debugging is enabled
The log4j.properties file for the method server will control advanced logging and debugging.

Example arguments:
    List: administratorEmail=admin@myDomain.com
    inputDirectory=C:\Temp\input
    debug=TRUE

IM_ExternalSelectionListSync

The IM_ExternalSelectionListSync method is involved with Gimmal external selection list synchronization. If the options for Gimmal selection lists are to be synchronized with data from another master or source system, this method will be configured to read data files from a specific directory and update Gimmal with data from that file. See "IM_ExternalSelectionListSync" on page 45.

Arguments: administratorEmail – this is the email address which will receive error notifications
inputDirectory – this is the directory that will contain data files from the source system. Files dropped into this folder will be read, processed, and then deleted. **Do not use this directory for any other purpose or use an existing directory with required files.**
Debug – a basic flag indicating whether basic debugging is enabled
The log4j.properties file for the method server will control advanced logging and debugging.
Example arguments:
    List: administratorEmail=admin@myDomain.com
    inputDirectory=C:\Temp\input
    debug=TRUE

IM_FetchExternalData

The IM_FetchExternalData method is involved with Gimmal external data lookup. This is an example method for lookups created for use in automated templates. Customer lookups should copy the configuration for this method and modify the copy to reflect the specific implementation details.

Arguments: docbase – the repository on which to perform the operation
installOwner – the repository installation owner id, used to carry out the operation
methodName – the name of the method to invoke
autoNumber – the auto-number assigned to the object for which data is being retrieved
Debug – a basic flag indicating whether basic debugging is enabled
Other parameters may be added/needed for client implementations.

IM_HTMLSenderLegal

The IM_HTMLSenderLegal method is involved with Gimmal e-mail notification. This method generates and sends email notifications for Gimmal tasks. It is invoked as a delegate method from dm_event_sender.

Arguments: Debug – a basic flag indicating whether basic debugging is enabled.
The log4j.properties file for the method server will control advanced logging and debugging. See also the documentation for dm_event_sender for a full list of arguments.

IM_MethodDataCleanup

The IM_MethodDataCleanup method is involved with Gimmal external method data cleanup. If external lookups are performed for automated templates, data are stored in im_method_data objects. These objects are dated at creation and persist in the repository for up to a week for help in debugging any interface issues. After that time, this method will delete those old objects, allowing the space to be reused. See "IM_MethodDataCleanup" on page 45.

Arguments: Debug – a basic flag indicating whether basic debugging is enabled.
The log4j.properties file for the method server will control advanced logging and debugging.

IM_Process Attributes

The IM_ProcessAttributes method is involved with Gimmal attribute processing. This method is a hook point for client specific metadata processing. This method may carry out a number of operations ranging from filing documents to setting metadata fields to applying permissions based on metadata values. The default implementation performs no processing; it simply returns. See "IM_ProcessAttributes" on page 45.

Arguments: docbase – the repository on which to perform the operation
installOwner – the repository installation owner id, used to carry out the operation
objectId – the object ID on which to perform the operation
Debug – a basic flag indicating whether basic debugging is enabled.

IM_ProcessAutofile

The IM_ProcessAutofile method is involved with Gimmal Auto File processing. This method is provided such that client workflows can invoke the Gimmal code to perform an autofile operation.

Arguments: documentNumber (required) – the auto number applied to the document to be filed
documentOnly (optional, default=false) – true if only the document should be filed, or false if its attachments should be filed as well
applyAutoFileACL (optional, default=true) – true or false, whether the configured auto file ACL should be applied
applyParentPermissions (optional, default=system parameter for Apply Parent Permissions) – whether the document permissions should be applied to its attachments
Debug – a basic flag indicating whether basic debugging is enabled.
The log4j.properties file for the method server will control advanced logging and debugging.

IM_ProcessChecklists

The IM_ProcessChecklists method is involved with Gimmal Checklist item processing. This method sends any necessary reminder messages about checklist items that have been assigned and not yet completed. This method utilizes the Gimmal "Notification Resend Interval" to determine how often to send messages as well as the 'Notification Resend Limit' parameter in order to determine at what point to no longer send nag messages. See "IM_ProcessChecklists" on page 45.

Arguments: Debug – a basic flag indicating whether basic debugging is enabled.
The log4j.properties file for the method server will control advanced logging and debugging.

IM_ProcessForms

The IM_ProcessForms method is involved with Gimmal Forms data input. If Gimmal Forms is configured to capture requests from end users, this method will import those request documents into Gimmal and set their metadata accordingly. See .

Arguments: administratorEmail – this is the email address which will receive error notificiations
inputDirectory – this is the interface directory where Gimmal Forms will store its output. Files dropped into this folder will be read, processed, and then deleted. **Do not use this directory for any other purpose or use an existing directory with required files.**
Debug – a basic flag indicating whether basic debugging is enabled.
The log4j.properties file for the method server will control advanced logging and debugging.
Example arguments:
    List: administratorEmail=admin@myDomain.com
    inputDirectory=C:\Temp\input
    debug=TRUE

IM_ProcessObligations

The IM_ProcessObligations method is involved with Gimmal Obligation processing. This method sends messages about obligation items that are coming due and are not yet completed. This method utilizes the Gimmal 'Notification Resend Interval' to determine how often to send messages as well as the 'Notification Resend Limit' parameter in order to determine at what point to no longer send nag messages. See .

Arguments: Debug – a basic flag indicating whether basic debugging is enabled.
The log4j.properties file for the method server will control advanced logging and debugging.

IM_ProcessTicklers

The IM_ProcessTicklers method is involved with Gimmal Reminder processing. This method sends notifications for reminder items that are coming due and are not yet completed. This method utilizes the Gimmal 'Notification Resend Interval' to determine how often to send messages as well as the 'Notification Resend Limit' parameter in order to determine at what point to no longer send nag messages. See .

Arguments: Debug – a basic flag indicating whether basic debugging is enabled.
The log4j.properties file for the method server will control advanced logging and debugging.

IM_ProcessWatermark

The IM_ProcessWatermark method is involved with Gimmal watermark insertion and removal. This method is provided such that client workflows can invoke the Gimmal code to apply or remove a watermark from a document.

Arguments: objectId (required) – the object ID for the document to be signed
operation (optional) – the operation to be performed. The value of this must be either APPLY or REMOVE (ignoring case); if absent or in error, then APPLY will be assumed
watermark (required for apply) – the specific text to be presented in the document as a watermark. This text will be converted to upper case. This may be omitted if attribute is specified instead
attribute (optional for apply) – the attribute containing the text to be presented in the document as

a watermark. The text value in this attribute text will be converted to upper case. If watermark is specified, this parameter will be ignored

currentUser (optional) – the user who is invoking the operation; this will affect the displayed last update user.

IM_RenderPDF

The `IM_RenderPDF` method is involved with performing OCR scanning on non-searchable PDF documents.

Arguments

- **exportDirectory** (required) – The directory where non-searchable PDF files will be staged for processing.

- **importDirectory** (required) – The directory where the resulting searchable PDF files will be staged for importing back into the system.

- **batchSize** (optional) – The maximum number of files to send to the OCR processor. Default value is 10.

- **notificationEmail** (optional) – If this argument is specified, an email is sent after the job completes indicating SUCCESS or ERROR. Separate multiple email addresses with a semicolon.

Example arguments

- exportDirectory \\datagateway\pdf_input_image

- importDirectory \\datagateway\pdf_output_searchable

- **notificationEmail admin@myDomain.com; admin2@myDomain.com**

IM_ScheduleDateReminders

The IM_ScheduleDateReminders method is involved with Gimmal date-based Reminder processing. This method, when executed with a provided object id, will update the automated (system-generated) reminders for a specific object in accordance with the business-defined rules. Reminders generated by this method can then be processed by IM_ProcessTicklers. See "IM_ScheduleDateReminders" on page 46.

Arguments: docbase – the repository on which to perform the operation
installOwner – the repository installation owner id, used to carry out the operation, objectId – the object ID for which to update automatic reminders
Debug – a basic flag indicating whether basic debugging is enabled.

IM_UnlockDocument

The IM_UnlockDocument method is involved with Gimmal document unlocking. This method provides members of the Gimmal_admin role the capability to cancel other users' checkouts. Typically this capability is restricted to System Administrators; Gimmal provides this enhanced capability so that the business users can manage this without having to call an administrator.

Arguments: docbase – the repository on which to perform the operation
installOwner – the repository installation owner id, used to carry out the operation
objectId – the object ID on which to perform the operation
Debug – a basic flag indicating whether basic debugging is enabled.

IM_UpdateUser

The IM_UpdateUser method is involved with Gimmal user ownership reassignment. This method provides administrators a means to reassign ownership of Gimmal objects from one user to another.

Arguments: fromUser – the user to be reassigned
toUser – the new user name
obligationOwner – whether to reassign Obligations owned by fromUser
obligationNotifyUser – whether to reassign Obligation notifications assigned to fromUser
reminderOwner – whether to reassign Reminders owned by fromUser
reminderNotifyUser – whether to reassign Reminder notifications assigned to fromUser
checklistAssignedUser – whether to reassign Checklist tasks assigned to toUser
checklistAssignedByUser – whether to update the user who assigned a Checklist task
checklistNotifyUser – whether to update the user to be notified about a Checklist task completion/rejection
legaltypes – whether to reassign ownership of Gimmal objects such as documents
Debug – a basic flag indicating whether basic debugging is enabled.
The log4j.properties file for the method server will control advanced logging and debugging.

IM_VersionInfo

The IM_VersionInfo method is involved with Gimmal server versions. This method is provided as an informational utility for Gimmal support. When executed, it will collect information on specific versions of files running on the method server. See "IM_VersionInfo" on page 46.

Arguments: Debug – a basic flag indicating whether basic debugging is enabled.
The log4j.properties file for the method server will control advanced logging and debugging.

Executing Jobs

Jobs are scheduled to run automatically or manually from within the Documentum Administrator.

Select a Job for Immediate Execution

1 Open the Documentum Administrator.

2 Expand the **Administration > Job Management > Jobs** folders.

3 Select Gimmal from the filter drop-down list on the right side of the window. See Figure 4-1.

Figure 4-1 List of Gimmal Contract Jobs

4 Right-click a job name, then select **Run**.

Recommended Maintenance Job Settings

Job warnings and notifications can be monitored from within an Administrator's Documentum standard e-mail inbox. This section details suggested Documentum job schedules running for Gimmal Contract, their purpose, and how they can be monitored.

Gimmal jobs to activate with suggested run intervals and arguments are in Table 3.

Table 3   Suggested Gimmal Contract Maintenance Job Settings

Job Name	Run Interval	Arguments
dm_AuditMgt	Once per month at night	Use default
dm_ContentWarning	Once per week at night	Use default
dm_DMClean	Once per week at night	Set "-clean_now TRUE"
dm_DMFilescan	Once per week at night	Set "-scan_now TRUE"
dm_LogPurge	Once per week at night	Set "-cutoff_days 15"
dm_QueueMgt	Once per week at night	Set "-cutoff_days 7"
dm_StateOfDocbase	Nightly	Use default
dm_UpdateStats	Once per week at night	Use default
IM_External DataSync	As required	IM_External DataSync
IM_ExternalSelectionListSync	As required	IM_ExternalSelectionListSync
IM_MethodDataCleanup	Nightly	IM_MethodDataCleanup

Table 3   Suggested Gimmal Contract Maintenance Job Settings (continued)

Job Name	Run Interval	Arguments
IM_ProcessAttributes	Never scheduled	IM_ProcessAttributes
IM_ProcessChecklists	Nightly	IM_ProcessChecklists
IM_ProcessForms	As required	IM_ProcessForms
IM_ProcessObligations	Once per day	IM_ProcessObligations
IM_ProcessTicklers	Once per day	IM_ProcessTicklers
IM_ScheduleDateReminders	Nightly	IM_ScheduleDateReminders
IM_VersionInfo	Never scheduled	IM_VersionInfo

Refer to current standard Documentum jobs and settings. See the Documentum Administrator Guide.

Extending Job End Date and Time

The Job Properties - Schedule Tab of each Job includes an End Date And Time field. Normally, this field is set for some years in the future. However, eventually the End Date will be reached, and the Job will no longer execute at the scheduled time(s), disabling the Gimmal Contract functionality which this expired Job controls.

Extend Job End Date and Time

1 Open the Documentum Administrator and expand the **Administration > Job Management > Jobs** folders.

2 Right-click the Job and select Properties.

3 Click the **Schedules** Tab.

4 In End Date And Time, select a one-time End Date and exact time or select after how many times the Job will end. See Figure 4-1.

Figure 4-1 Job End Date Expiration

5 Click OK. If the selected date is anytime in the future, the Job will continue to run until that end date and time.

Viewing Output Reports from Custom Gimmal Contract Jobs

If tracing level is set > **0** for a specific job, an associated report will be saved to a repository folder. This report provides valuable debugging information if a job problem is suspected.
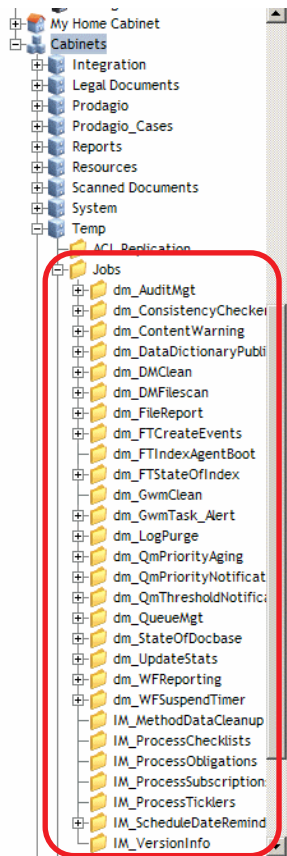
View Output Reports from Gimmal Contract Jobs

1 Click Tools, then select **Preferences.** The Preferences General window displays**.**

2 On the General tab, check ☑ **Show hidden objects**. See Figure 4-1.

Figure 4-1 Documentum Preferences
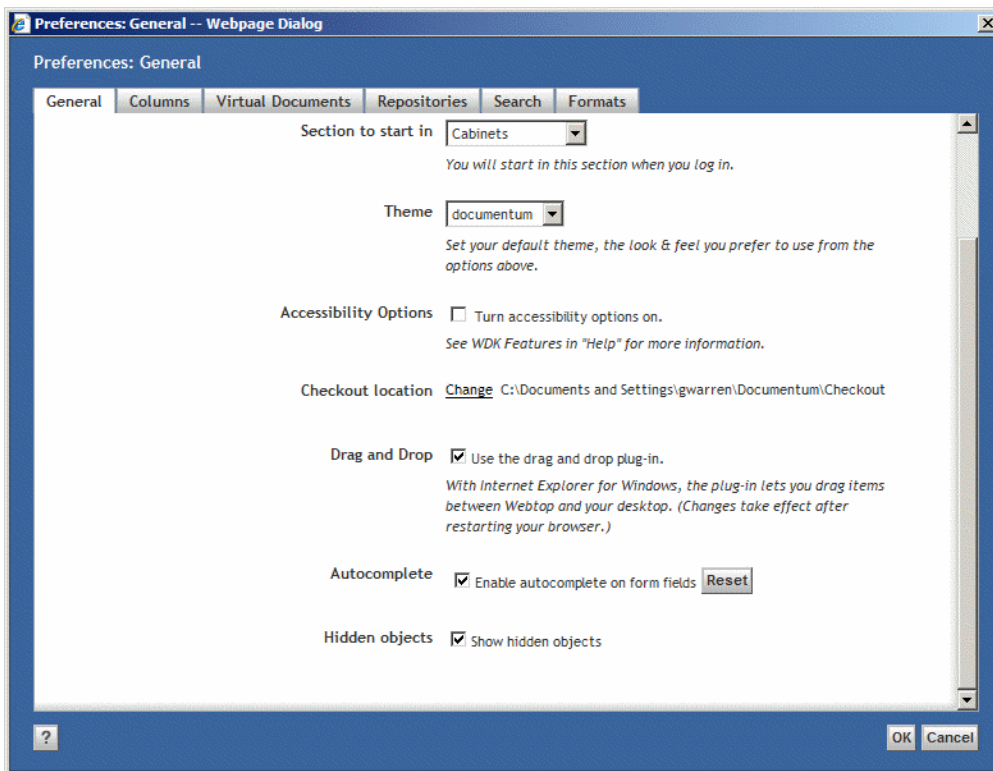
3 Click OK .

4 Navigate to the Cabinets >Temp >Jobs folder. See Figure 4-1.

Figure 4-1 Job Reports location

5 Select the job name to review its reports. The job reports listing displays. See Figure 4-1.

Figure 4-1 Reports Listing

6 From the list of reports, double-click the report name to display the report.

More detail: Click the **Modified** column header to display the newest records at the top of the list.

Jobs Related to Workflow Administration

Running workflows within Gimmal Contract utilizes standard Documentum infrastructure. Please consult EMC Documentum's support website and documentation.

The Queue Management tool deletes de-queued Documentum Inbox items. If standard Documentum inbox processing becomes a frequent activity and de-queued items are not deleted, the tables for the **dmi_queue_item** type can grow quite large and performance may degrade.

The queue management tool generates a status report that provides a list of the deleted dmi_queue_items. The report is saved in the Docbase in the folder **/System/Sysadmin/Reports/QueueMgt**.

Implementing Security

This chapter includes the following topics:

Maintenance of Users And Roles

Overview

Gimmal Contract Management allows easy maintenance of users and roles. All user maintenance actions are provided through the standard User Management area on the System Administration pane of the Documentum Administrator (DA) tool.

Adding and Managing Users

Users are added and managed using the Documentum Administrator. See the *Documentum Administrator Users Guide* and see .

Gimmal Contract Management uses standard Documentum user administration. The following notes are specific to the Gimmal Contract Management application behavior.

- A minimum Extended Privilege level of View Audit is necessary for a user to view the Gimmal Audit trail.

- Client Capability Settings
    — Consumer: *Read Only* access to all documents and related data
    — Contributor: Can add and modify documents and related data
    — Coordinator: Same as Contributor
    — System administrator: Same as Contributor except the **Show all properties** option is available on the properties edit/display page. Also allows access to Admin tasks and features in Documentum Administrator (DA).

- Gimmal Administrator Role

    Users who are members of the Gimmal_admin role have access to the Admin components of Gimmal Contract Management. The features controlled by the Gimmal_admin role are described in the *Gimmal Contract Management 6.9.1 Business Administrator Guide*.

Table 4   Sample Roles

Contract Analyst
Legal Reviewer
Gimmal_admin
Gimmal_type_reviewer
Gimmal_contact_admin
Gimmal_time_manager

Gimmal_admin
This role is created during the installation process. Members of the **Gimmal_admin** role have special access privileges and are typically given full rights in all Product Name permission sets.

Gimmal_type_reviewer
This role is typically used in conjunction with a scan server. Users in this role are allowed to change the type of a document from a generic type im_scanned to a more specific (often contractual) type. Users not in this role are not allowed to perform such type-changing operations.

Gimmal_contact_admin
This role enables users to maintain the Gimmal Global Contacts list. Users not in this role may read and relate to entries in the global contacts list, but may not edit them.

Gimmal_time_manager
This role allows users to lock and unlock time entries created by other users. This prevents unauthorized changing of such items as billable time.

Creating Users and Groups

Gimmal Contract Management uses the standard Documentum permissions when creating or modifying a new user or group

Creating a New User

This task describes the process of creating a new user for Gimmal Contract Management.

Create a New User

1 In the **Administration** pane under **User Management**, click **Users**. The Users window displays.

2 Click File, then select New > User. The New User window displays. See Figure 5-1.

Figure 5-1 Create New User

3 Use the settings in Table 5 to set up the new user.

Table 5   User Settings
Table 6

State	Select Active or Inactive (Inactive disables login)
Name	User name as it will appear in Gimmal Contract Management
User Login Name	User name as it will display for Login (may be the same as Name)
User Source	Default to **None**. Or select LDAP or Inline Password.
Description	Optional
email Address	User email address
User OS Name	User account in the operating system
Windows Domain	User account domain
Home Repository	Defaults to current docbase
Default Folder	Defaults to **Choose/Create folder with the user name**
Default Group	Not selected
Default Permission Set	Not selected
Db Name	Leave blank
Privileges	Set to **None** for most users. Superusers can be given more privileges.
Extended Privileges	Set to **View Audit** if the user is allowed to view the Audit Trail. Otherwise, set to **None**.
Client Capability	Set to **Consumer** for read-only users Set to **Contributor** or **Coordinator** for users who will author **documents** Set to **System Administrator** for **Superusers**
Alias Set	Set default to **None Selected**

4 Click **OK**. The new user is created.

Differences between System Administrator and Superuser

The user with System Administrator privileges can:

- Create, alter, and drop users and groups.
- Create, modify, and delete system-level ACLs.
- Grant and revoke Create Type, Create Cabinet, and Create Group privileges.
- Create types, cabinets, and printers.
- Manipulate workflows or work items, regardless of ownership.
- Manage any object's lifecycle.
- Set the a_full_text attribute.

The System Administrator privilege does not override object-level permissions.

The user with Superuser privileges can:

- Perform all the functions of a user with System Administrator privileges.
- Unlock objects in the repository.
- Modify or drop another user's user-defined object type
- Create subtypes that have no supertype
- Register and unregister another user's tables
- Select from any underlying RDBMS table regardless of whether it is registered or not
- Modify or remove another user's groups or private ACLs
- Create, modify, or remove system ACLs
- Grant and revoke Superuser and System Administrator privileges
- Grant and revoke extended privileges
- View audit trail entries

Modifying an Existing User

This task describes the process for modifying an existing Gimmal Contract Management user profile information.

Modify User Profile Information
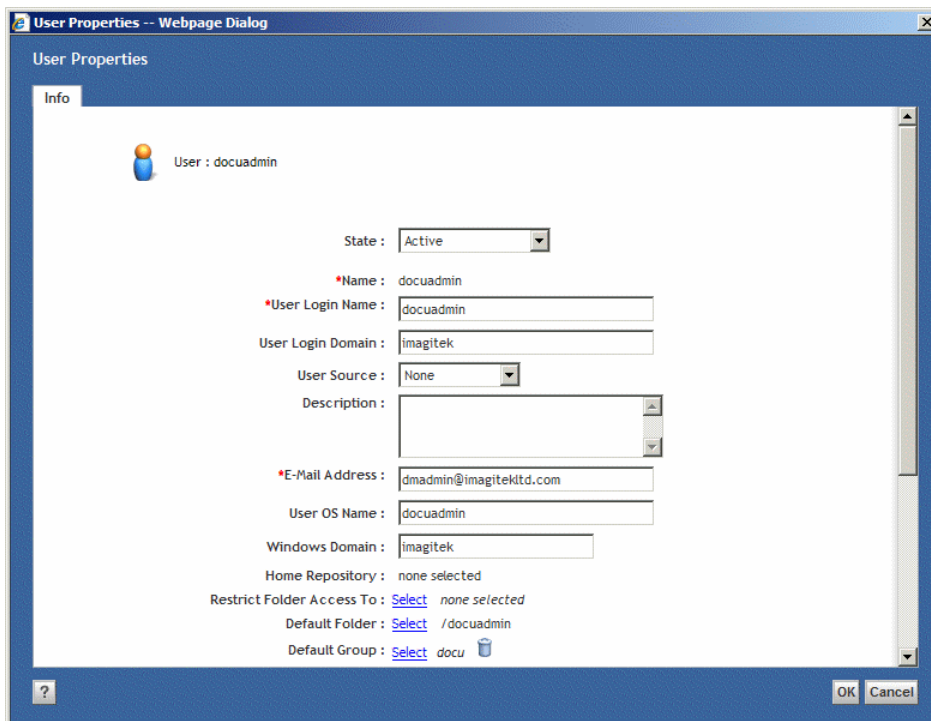
1 In the Administration pane under User Management, click Users. The Users window displays. See Figure 5-1.

Figure 5-1 User Search Window

2 Enter the needed user name and click **Search** and locate the user.

3 Right-click the user name and select Properties. The User Properties window displays. See Figure 5-2.

Figure 5-2   Modify User

4 Modify fields as necessary.

5 Click **OK**. The selected user is modified.

Renaming a User

This task describes how to rename an existing user when the user has changed their name for any reason.

Rename an Existing User

Before beginning

First, reassign all Gimmal special objects. See the separate *Gimmal 6.9 Business Administrator Guide*.

1 In the Administration pane under User Management, click Users. The Users window displays. See Figure 5-1.

Figure 5-1 User Search
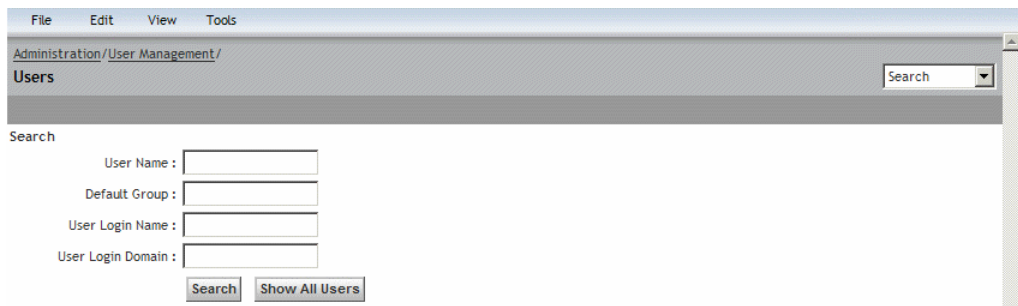
2 In User Name, enter the user name. The user name displays.

3 Right-click the user name and select Reassign User. The Reassign User window displays. See Figure 5-1.

Figure 5-1 Reassign User
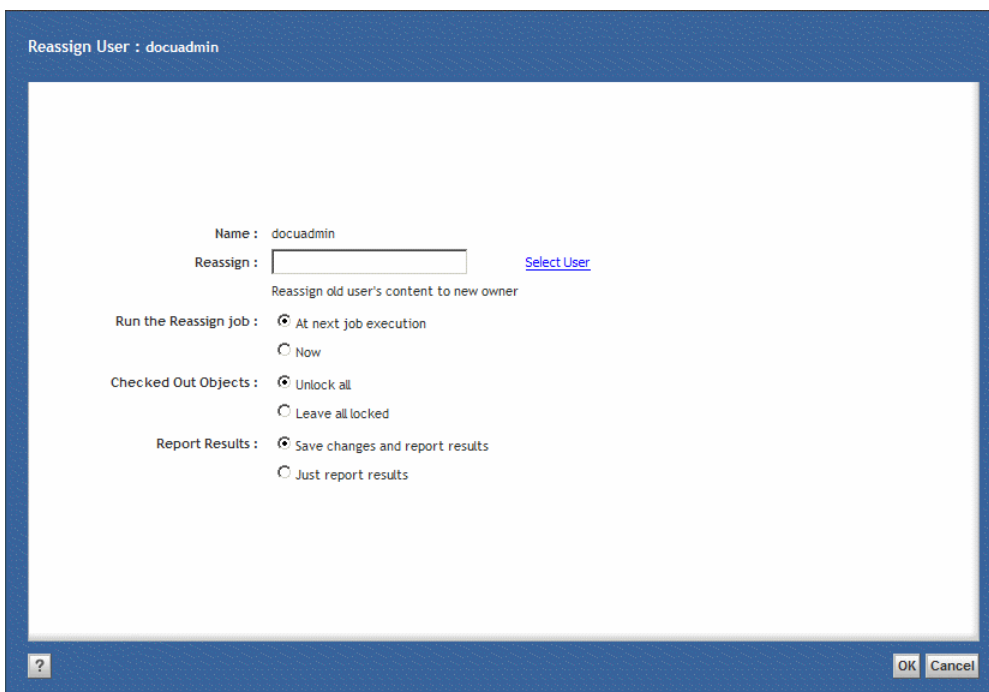
4 In **Reassign**, enter the new name for the user.

5 For **Run the Reassign job**, select At next job execution.

6 Click OK. All instances of the previous name are replaced with the newly assigned name at the next job execution.
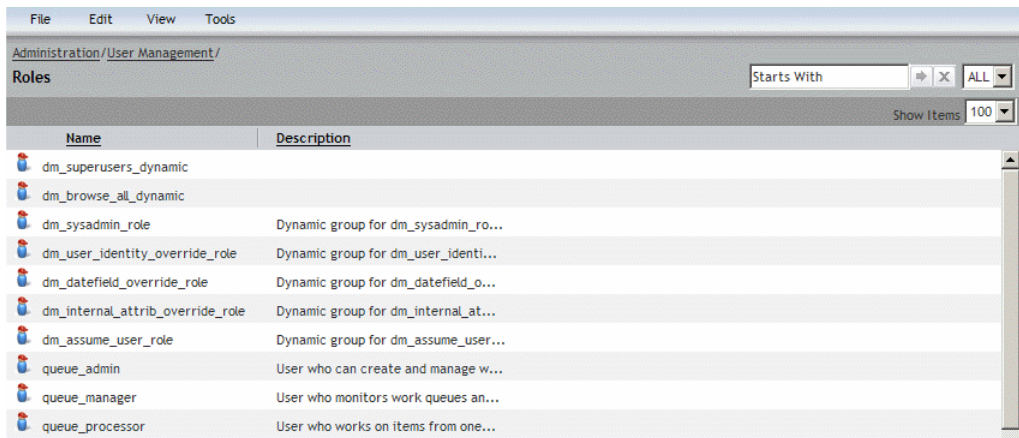
Assigning Role/Group Membership

After configuring user profiles, add each of the users to a Gimmal Contract Management role or group. The roles and groups will vary based on business requirements.
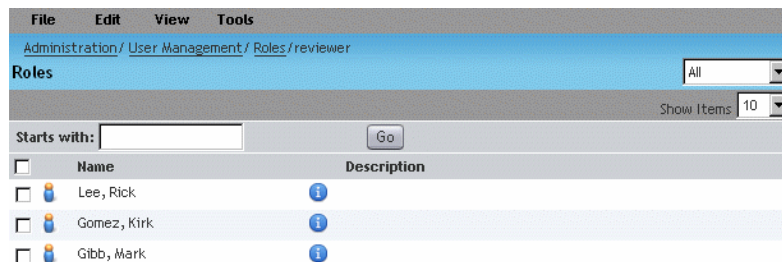
View or Modify Role/Group Membership

1 In the **Administration** pane, click **User Management,** then click **Roles**. The Roles window displays all available roles. See Figure 5-1.

Figure 5-1 Roles

2 Right-click a role name, then select View Current Group Memberships. The role's current membership displays. See Figure 5-1.

Figure 5-1 Role Memberships

3 Repeat these steps to view Group memberships, substituting Role for Group.

4 To add a new role or group member, display the user name.

5 Right-click, then select Assign Group Membership. The Choose a group window displays. See Figure 5-1.

Figure 5-1 Choose a Group
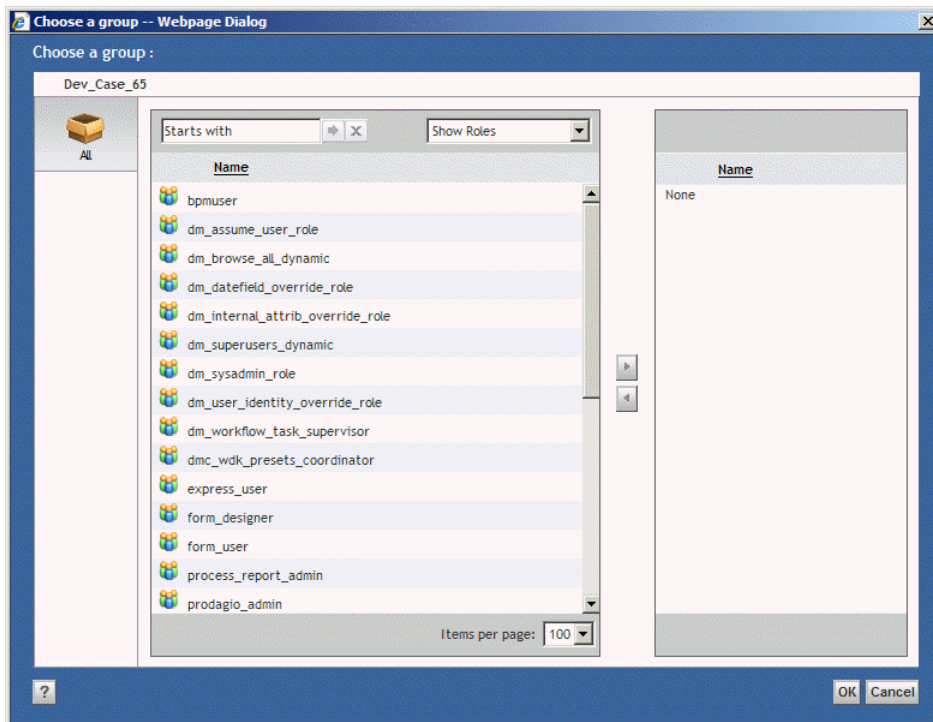
6 In the Show Groups and Roles menu, select Show Groups and Roles.

7 To add a user to a role, select the user(s) to add to the role from the left **Name** column and click
   [▶].

More detail: Add a group in the same way as adding a role. Simply choose the group name instead of the
role name.

8 Click [OK]. The selected user is a member of the selected role or group.

Creating a User Role

Gimmal Contract Management allows roles to be added that support any business context.

Create a New User Role

1 In the **Administration** pane, click **User Management,** then click **Roles**. The Roles window
   displays all available roles. See Figure 5-1.

2 Click **File, t**hen click **New,** then click **Role.** The New Role window displays. See Figure 5-1.

Figure 5-1 New Role

3 In **Name**, enter a name for the new role.

4 Leave the **email Address** blank.

5 Click OK . The new role is created.

Product Name Security Model

Product Name is designed to use standard Documentum security model capabilities. Access to features and components is controlled by permission sets, group/role membership, and settings in the user profiles.

This chapter conceptually describes how Gimmal Contract Management implements and uses the Documentum security model. Please consult Documentum security documents for detailed procedures.

Managing Security

Security is managed with Documentum permission sets. Use the Documentum Administrator to set up security schemes for the Gimmal Contract Management repository.

See the *Protecting Repository Object* section in the *Documentum Content Server Administrator's Guide*.

User Profile Settings

A user profile is created for each user that will access Product Name. The profile contains login information as well as user level access permissions. See the "Permission Sets" on page 73 for more detail.

Roles

Users are assigned to various roles for security access. Roles are named groups that can be defined for any business scenario. See the *Gimmal Contract Management 6.9 User Guide* for more information on these functions.

Permission Sets

A permission set determines who can access a particular object in a repository. Each object in the repository has an associated permission set, determining who can access the object and what actions each user (role) can perform. Access to a repository object is determined by the permission set assigned to the object.

A permission set lists the roles that have access. The permission set assigns one of the following seven access levels to each user and group listed. Each access level includes all the permissions of the preceding levels (is hierarchical):

- **None** – no access to the object is permitted
- **Browse** – users can view the object's properties (but not the object's content)
- **Read** – users can view both the properties and the content of the object
- **Relate** – users can do the above and add annotations to the object
- **Version** – users can do the above and modify the object's content and check in a new version of the item (with a new version number). Users cannot overwrite an existing version or edit the object's properties.[
- **Write** – users can do the above and edit object properties and check in the object as the same version
- **Delete** – users can do all the above and delete objects

The following table displays a sample permission set. Two special permission groups (Owner and World) are set for each permission set. The Owner is the user who created the object. World is any user with an active user profile in the docbase.

Table 7   Sample Permission Set

Table 8

Job Role	Access Permission
author	Write
reviewer	Version
approver	Read
Owner	Browse
World	None

More detail: Users who have membership in multiple roles will be granted the most permissive access rights.

See the *Documentum Administrator Users Guide* for a complete description of permission sets.

Controlling User Access to Cabinets

Gimmal Contract Management allows easy display or hiding of specific cabinets to users. Often, hiding cabinets such as System and Temp to prevent users from seeing those cabinets is needed.

Create the Gimmal Admin Role (If Needed)

In order for all Gimmal Contract Management features and functionality to be enabled:

- Ensure that the Gimmal_admin role has been added to the repository.
- Ensure that the History cabinet allows world write access.

The Gimmal_admin role allows users to access Administrator components. It also enables various features within the repository that depend on the role to operate correctly.

If the Gimmal_admin role is not present in the docbase, it can be created using Documentum Administrator.

Create the Gimmal_admin Role

1 Select **User Management**, click **Roles**, and then click **New**

2 Click **Role**. See "Create a New User Role" on page 70.

3 In **Name**, enter **Gimmal_admin**.

4 Click **OK**. The new role is created. It is unnecessary to assign users to the role.

Hiding or Displaying Cabinets

Each Cabinet can be hidden from or displayed to users.

Hide a Cabinet

1 Click **Cabinets**. The Cabinets window displays.

2 Right-click a Cabinet name and select **Properties**.

3 Select **Show all properties**. Additional properties display.

4 Scroll down and select **Hidden**.

5 Click **OK**. The Cabinet is hidden from view.

More detail: Role and Group access to Cabinets may be controlled using permission sets. See "Product Name Security Model" on page 72.

Role and Group access to Cabinets can be controlled using permission sets ("Permission Sets" on page 73).

Display a Cabinet

1 Click **Cabinets**. The Cabinets window displays.

2 Right-click a Cabinet name and select **Properties**.

3 Select **Show all properties**. Additional properties display.

4 Scroll down and deselect **Hidden**.

5 Click **OK**. The Cabinet is displayed.

Create a Home Cabinet for LDAP Users

This mapping process creates a cabinet for each LDAP user as each user is added to the repository. The cabinet is owned by the user and is the private home cabinet of that user.

1 From the LDAP Server Configuration Properties Mapping tab, add:

- **Property: default_folder**
- **Type: dm_user**
- **Map To: /${cn}**
- **Map Type: Expression**

Document Types and Attributes

Once an organization has implemented Gimmal Contract Management, it is not unusual for the organization to expand upon that investment by using Gimmal Contract Management in other parts of their organization. This chapter describes the basic concepts and procedures in the process of adding new document types to the Documentum repository for use with Gimmal Contract Management.

ALERT! Only individuals trained in using Documentum Application Builder (DAB) should perform functions and actions in this chapter.

Core Document Types

As part of its security model, Gimmal Contract Management uses a few selected types to provide the core of its functionality. These types are im_legal_attachment, im_legal_document, im_legal_request and im_legal_scorecard. Gimmal document types are prefixed with im_. Documentum document types are prefixed with dm_.

Documents derived from im_legal_document are typically referred to as *Principal Documents* by Gimmal Contract Management. These documents are used in hierarchies of documents and provide the greatest amount of power and flexibility within the system. Most types of documents kept within Gimmal will be a subtype of im_legal_document and make use of these exceptional features.

Documents derived from im_legal_attachment are used as supporting documents or attachments for other documents in the system. These documents cannot have attachments to them and have a restricted set of features, and usually include items such as a personnel photo or application form that will not have an extensive life cycle or business function to be managed.

Documents derived from im_legal_request represent a kind of external request from another department. These documents carry no legal weight or significance of their own; they are simply a request for some action to be performed by another corporate entity. These documents have their own set of features, but **cannot** be included in a structure of related documents.

Table 9 is a listing of the standard Gimmal document types and attributes used in Gimmal Contract Management. Edit data in this table with Documentum tools or with typical database editor tools, such as SQL.

Table 9   Gimmal Contract Management Types and Attributes

SQL tables ending in _s are tables that are storing single value; _r denotes multi (repeating) values. Types that use both single and multi-values are associated with two tables.

Type Name	SQL Table	Attribute Name	Attribute Description
im_admin_audit	im_admin_audit_r	im_event	Event
	im_admin_audit_s	im_event_data_1	Event Details 1
		im_event_data_2	Event Details 2
		im_event_data_3	Event Details 3
		im_event_data_4	Event Details 4
		im_event_data_5	Event Details 5
		im_event_time	Date/Time
		im_event_user	User

		im_object_type	Object Type
im_automated_template	im_automated_template_s	document_description	Description
		document_number	Document Number
		document_title	Title
		has_tickler	Has Tickler
		template_category	Category
		template_document_type	Template Type
im_config_autofile	im_config_autofile_r im_config_autofile_s	apply_acl_name	Permission Set to Apply
		example_path	Example Path
		object_type	Object Type
		path_parameters	Path Parameters and Order
im_config_autoname	im_config_autoname_r im_config_autoname_s	name_suffix	AutoName Suffix
		object_type	Object Type
		set_title_field	Set Title Field?
		suffix_example	AutoName Example
im_config_autonumber	im_config_autonumber_s	last_number	Last Number
		min_digits	Minimum Numeric Digits
		object_type	Object Type
		prefix	Prefix
		suffix	Suffix
im_config_checklist	im_config_checklist_s	allow_clear	Allow Clear
		attr_name	Attribute Name
		attr_value	Attribute Value
		description	Description
		list_category	List Category
		list_name	List Name
		list_type	List Type
		modified_date	Modified Date
		sequence_number	Sequence Number
		signoff_required	Signoff Required
		task_name	Task Name
im_config_comp_access	im_config_comp_access_s	access_allowed	Access Allowed
		component_id	Component
		object_type	Object Type
		user_role	User Role
im_config_date_re-minder	im_config_date_reminder_r im_config_date_reminder_s	action	Reminder Action
		date_field	Date Field
		days_advance	Days Advance Notice
		distribution_list	Distribution List
		is_revised	Revised
		message	Message
		object_type	Object Type
		reminder_name	Reminder Name
im_config_external_system	im_config_external_system_r im_config_external_system_s	base_url	Base URL
		param_name	Parameter Name

		param_value	Parameter Value
		scope	Scope
		system_lbl	System Label
im_config_jacket	im_config_jacket_s	attribute_name	Attribute Name
		object_type	Object Type
		sequence_number	Sequence Number
im_config_report	im_config_report_s	enabled	Enabled
		report_category	Report Category
		valid	Valid
im_config_system	im_config_system_s	allow_edit	Allow Edit
		parameter_name	Parameter Name
		parameter_value	Parameter Value
im_config_type_access	im_config_type_access_s	access_allowed	Access Allowed?
		object_type	Object Type
		user_role	Group/Role
im_config_ui_legal_text	im_config_ui_legal_text_s	ui_location	UI Location
im_date_reminder	im_date_reminder_s	action	Action
		comments	Comments
		completion_date	Completed Date
		completion_user	Completed By
		creation_date	Creation Date
		distribution_list	Distribution List
		instructions	Instructions
		notification_date	Notification Date
		object_type	Object Type
		priority	Task Priority
		queue_date	Queue Date
		recurring	Recurring
		reminder_name	reminder_name
		status	Status
		tracking_number	Tracking Number
im_legal_attachment	im_legal_attachment_r im_legal_attachment_s	document_category	Category
		document_number	Document Number
		document_status	Status
		document_title	Document Title
		external_clauses	External Clauses
		has_tickler	Has Tickler
		is_jacket_image	Show Image on Jacket?
		jacket_sequence_number	Jacket Sequence Number
		originating_template	Originating Template
		tracking_number	Tracking Number
im_legal_checklist	im_legal_checklist_s	allow_clear	Allow Clear
		assigned_by_user	Assigned By
		assigned_date	Date Assigned
		assigned_user	Assigned To
		attr_name	Attribute Name
		attr_value	Attribute Value

		complete_comment	Completion Comment
		complete_time	Completed Date
		complete_user	Complete User
		created_date	Date Created
		description	Description
		due_date	Due Date
		list_category	List Category
		list_name	List Name
		list_type	List Type
		notify_user	Notify When Complete
		object_type	Object Type
		priority	Priority
		queue_date	Queue Date
		reject_comment	Rejection Comment
		reject_status	Rejection Status
		sequence_number	Sequence Number
		signoff_required	Signoff Required
		task_name	Task Name
		tracking_number	Tracking Number
im_legal_clause	im_legal_clause_s	document_category	Category
		document_description	Description
		document_number	Document Number
		document_title	Document Title
		fallback_clause	Fallback Clause
		has_tickler	Has Tickler
		risk_level	Risk Level
im_legal_contact	im_legal_contact_s	address_1	Address 1
		address_2	Address 2
		cell_phone	Cell Phone
		city	City
		contact_id	Contact ID
		contact_title	Title
		contact_type	Contact Type
		country	Country
		email	Email Address
		fax	Fax
		first_name	First Name
		full_name	Full Name
		home_phone	Home Phone
		last_name	Last Name
		organization	Organization
		state_code	State/Province
		tracking_number	Tracking Number
		work_phone	Work Phone
		zip	Zip / Postal Code
im_legal_contact_ref	im_legal_contact_ref_s	contact_id	Contact ID
		tracking_number	Tracking Number

		contact_type	Contact Type
im_legal_document	im_legal_document_r	document_category	Category
	im_legal_document_s	document_date	Document Date
		document_number	Document Number
		document_status	Status
		document_title	Document Title
		external_clauses	External Clauses
		has_attachment	Has Attachment
		has_obligation	Has Obligation
		has_related	Has Related Documents
		has_tickler	Has Tickler
		master_document_number	Master Document Number
		originating_template	Originating Template
im_legal_history	im_legal_history_s	object_type	Object Type
		object_version	Object Version
		object_version_ts	Object Version Timestamp
		object_vstamp	Object VStamp
		tracking_number	Tracking Number
im_legal_note	im_legal_note_s	access_group	Access Restriction
		document_version	Version
		entry_category	Category
		entry_owner	User
		entry_text	entry_text
		entry_time	entry_time
		tracking_number	Tracking Number
im_legal_obligation	im_legal_obligation_r im_legal_obligation_s	amount	Amount
		category	Category
		comments	Comments
		completion_comments	Completion Comments
		completion_date	Completion Date
		completion_user	Completion User
		currency	Currency
		distribution_list	Distribution List
		due_date	Due Date
		financial	Financial
		instructions	Instructions
		location	Location
		notification_date	Notification Date
		object_type	Object Type
		priority	Task Priority
		queue_date	Queue Date
		recurring	Recurring
		responsibility	Responsibility
		series_id	Series ID
		status	Status
		sub_category	Sub Category
		tracking_number	Tracking Number

		unit_quantity	Quantity
		unit_type	Unit Type
im_legal_reference	im_legal_reference_s	document_category	Category
		document_description	Description
		document_number	Document Number
		document_title	Title
		has_tickler	Has Tickler
im_legal_request	im_legal_request_s	request_closed_date	Date Closed
		request_description	Description
		request_initiation_date	Date Initiated
		request_number	Request Number
		request_requestor	Requestor Name
		request_required_date	Date Required
		request_status	Status
		request_title	Request Title
		request_type	Request Type
im_legal_review	im_legal_review_s	document_version	Document Version
		entry_owner	User
		entry_text	Text
		entry_time	Time
		entry_type	Review Type
		tracking_number	Tracking Number
im_method_data	im_method_data_s	data_timestamp	Data Timestamp
		method_name	Method Name
		parameter_name	Parameter Name
		parameter_value	Parameter Value
		tracking_number	Object Number
im_selection_list	im_selection_list_s	list_key	List Key
		list_name	List Name
		list_value	List Value
		sequence	Sequence
im_standard_template	im_standard_template_s	document_description	Description
		document_number	Document Number
		document_title	Title
		has_tickler	Has Tickler
		template_category	Category
		template_document_type	Template Type
im_tickler_event	im_tickler_event_r im_tickler_event_s	action	Action
		comments	Comments
		completion_date	Completed Date
		completion_user	Completed By
		creation_date	Creation Date
		distribution_list	Distribution List
		instructions	Instructions
		notification_date	Notification Date
		object_type	Object Type
		priority	Task Priority
		queue_date	Queue Date

		recurring	Recurring
		status	Status
		tracking_number	Tracking Number
im_time_entry	im_time_entry_s	activity	Activity
		category	Category
		comments	Comments
		duration	Duration
		end_date	End Date
		start_date	Start Date
		status	Status
		subactivity	Sub-Activity
		timeentry_user	User
		tracking_number	Tracking Number

Creating New Document Types

When creating a new document type, first identify the document's purpose. Is it a primary document, an attachment or a request?

You can extend any of the types im_legal_attachment, im_legal_document, im_legal_request and im_legal_scorecard freely using Documentum Composer. Refer to Documentum Composer materials for details. For further options, contact Gimmal Support.

Refer to Documentum DA documentation for additional details.

Scanning Document Type

Gimmal Contract Management includes a document type named im_scanned. This document type is assigned to scanned documents.

After importing these scanned documents, the System Administrator reviews the scanned document and then changes it from a scanned document type to a more accurate document type. See "Core Document Types" on page 76 and Changing a Document Type in the *Gimmal Contract Management 6.9 Business Administrator Guide.*

Defining Property Page Layout

The ordering of attributes within the properties pages within Gimmal Contract Management is also controlled by Documentum, easily accessed from Documentum Application Builder (DAB).

Define Property Page Layout

1 Double-click the document type.

2 Click the Display Configuration tab.

3 Select application='webtop' in the Scope menu to affect what is displayed in Gimmal Contract Management. See Figure 5-1.

Figure 5-1 Display Configuration Tab
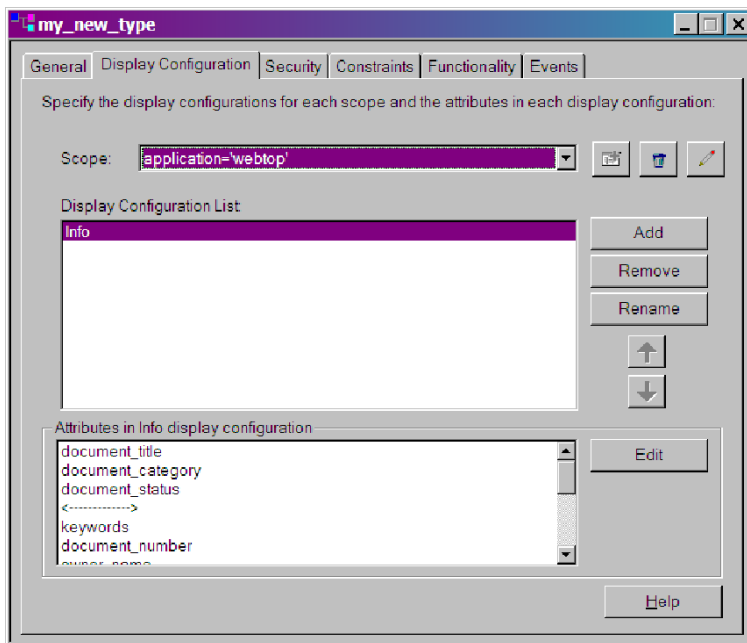
4 Continue editing this tab according to the instructions in the Documentum reference documentation.

Diagnostics

This chapter presents the following topics:

System Diagnostics

The System Diagnostics area of the System Administrator's window includes: managing Log4j properties, viewing the Java Virtual Machine (JVM) information, running DMCL traces and testing the SMTP server.

Manage Log4j Properties

The Log4j Properties file records each action taken by Java for subsequent troubleshooting.

1 Press and hold the **Ctrl** key and click the Admin icon. The Configuration Dashboard displays.

2 In the **System Diagnostics** section, click **Manage Log4j Properties**. The Manage Log4j Properties File window displays (Figure 6-1).

Figure 6-1 Manage Log4j Properties
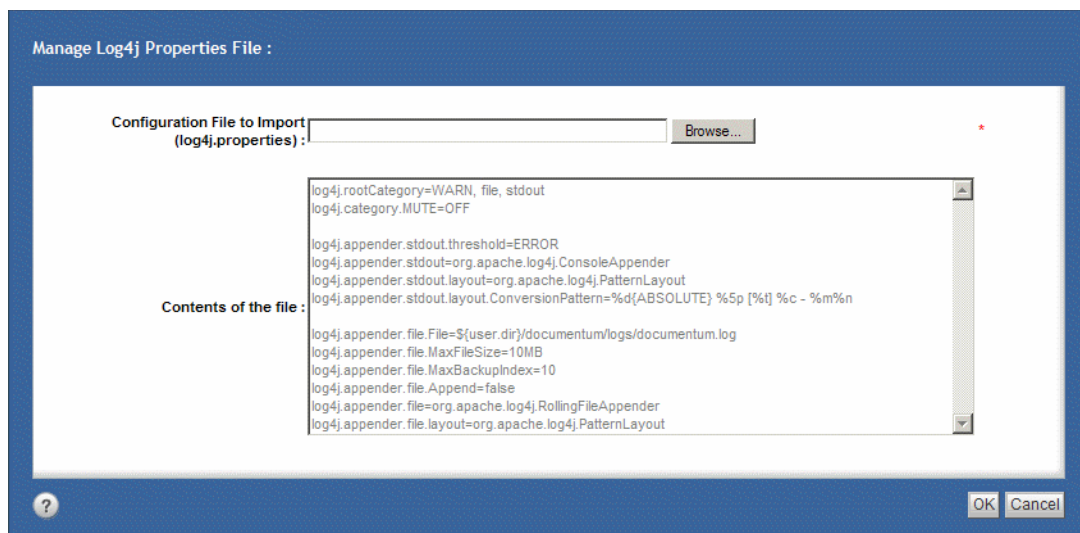
3 Click **Browse** to locate enter the **Configuration File to Import (log4j Properties)**. The contents of the selected file display.

4 Click **OK**. The selected log4j.properties files is imported.

View Java Virtual Machine Information

The Java Virtual Machine (JVM) information lists property names and their values and it includes the Run Time environment.

1 Press and hold the **Ctrl** key and click the **Admin** icon. The Configuration Dashboard displays.

2 In the **System Diagnostics** section, click **View JVM Info**. The JVM Info window displays (Figure 6-2).

Figure 6-2   JVM Window
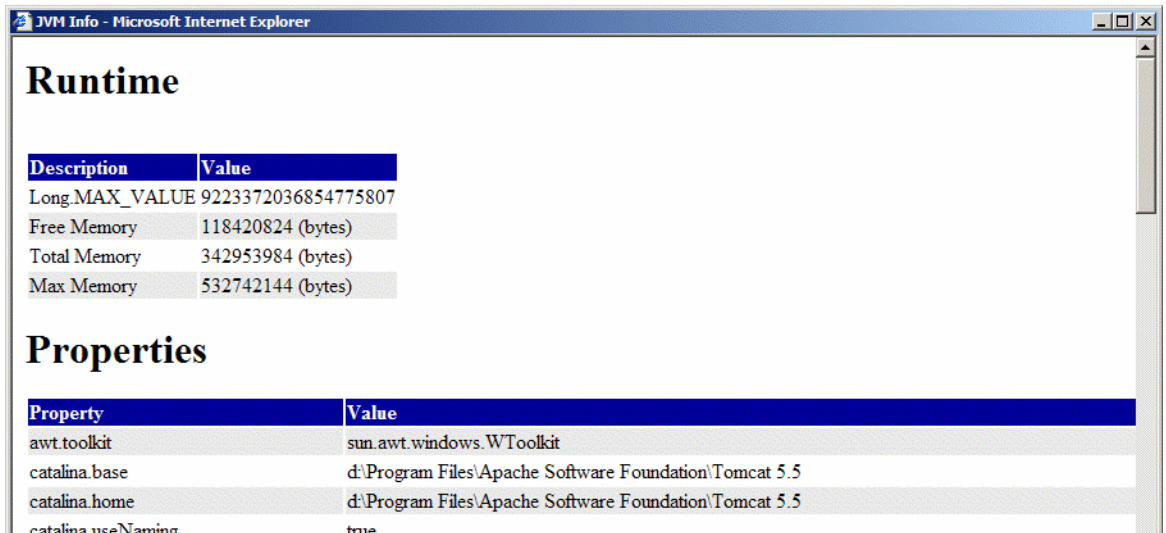
3 Close the JVM window.

Run the DMCL Trace

The Documentum Configuration Library lists the browser tracing for subsequent performance analysis and improvement.

1 Press and hold the **Ctrl** key and click the **Admin** button. The Configuration Dashboard displays.

2 In the **System Diagnostics** area, click **Run DMCL Trace**. The Browser DMCL trace window displays, with the trace off (Figure 6-3).

Figure 6-3   Browser DMCL Trace
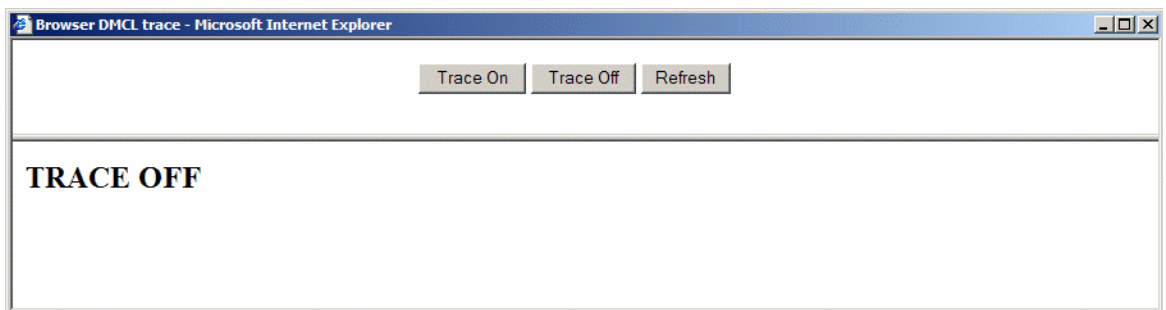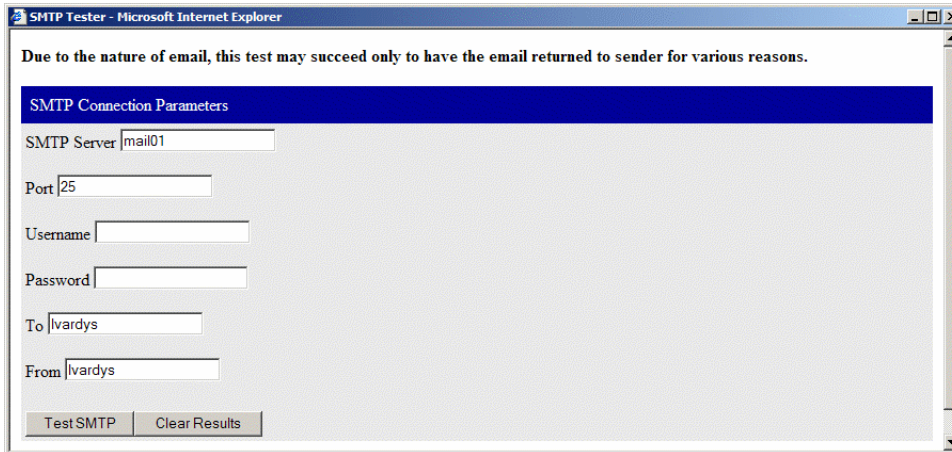
3 Click **Trace On**. TRACE OFF changes to TRACE ON.

4 Click **Refresh**. The trace displays.

5 Close the Browser DMCL Trace window.

Test the SMTP Server

The SMTP Server test confirms the accurate transmittal of emails, and lists details if the email was not sent, allowing troubleshooting.

1. Press and hold the **Ctrl** key and click the **Admin** button. The Configuration Dashboard displays.

2. In the **System Diagnostics** area, click **Test SMTP Server**. The SMTP Tester window displays. See Figure 6-1.

Figure 6-1 SMTP Tester

3. Complete all fields. Consult with a System Administrator, if needed.

4. Click **Test SMTP**. An attempt is made to send the email to the intended recipient.

5. Scroll to view the results at the bottom of the window.

6. (Optional) Troubleshoot and fix any error by clicking **Clear Results**.

7. Close the SMTP Tester window.

Method Server Log

The Method Server Log contain outputs of jobs running on the Method Server.

<DCTM_HOME>\jboss7.1.0\server\DctmServer_MethodServer\log

Application Server Log:

Per your application server documentation; for Tomcat

<TOMCAT_HOME>\logs

Content Server Log:

<DCTM_HOME>\dba\log\<Repository_Name>.log

There could also be a custom log as specified in the custom logging/diagnostic configuration (specified by the log4j.properties file). See *System Diagnostics - Logging Configuration* in the Documentum documentaiton for further information.

Troubleshooting CRTEXT Format Error

With some DTS and Documentum 6.7 clients, when Documentum cannot convert objects in the crtext format, it will display this error message because Documentum cannot automatically generate thumbnails, proxies, and metadata content in this format:

Task Description:
The Profile with object ID: 0821e301800365e1 and Name: register failed to execute for the document with object ID: and Name: Attribute History: Amendment to BKL (RELA-000164 v1.1).properties, Source Format: null, Source Page Modifier: , Target Format: null, Target Page Modifier: . See log file for details.

To resolve this error:

1 In DA, click **Formats** in the browser tree at the left.

2 Locate and click **richtext** in the list and open its Properties page.

3 Deselect **Rich Media: Generate thumbnails, proxies, and metadata** for content in this format.

4 Click **OK**.

5 Restart all relevant services.

Technical Support

The standard Gimmal Contract Management Maintenance subscription entitles 3rd level support through the support web site at http:upport.gGimmalimmal.com. Your in-house 2nd level support team should be able to field system issues with the native Documentum system prior to submitting a case with Gimmal Contract Management. This troubleshooting checklist will assist in determining the nature of the issue.

Table 10   System Issue/Application Checklist

Validate that the docbase can be successfully accessed through the Documentum Administrator and/or baseline WebTop client.	Documentum Technical Support
Validate that the Documentum Server and Docbroker logs are clean.	Documentum Technical Support
Check that the standard Documentum agent reports have no anomalies.	Documentum Technical Support
Verify that the Web Application Server hosting Gimmal Contract Management is currently running and check the log for errors.	Documentum Technical Support
Verify that the Gimmal Contract Management jobs are executing as expected and that the job reports are error free.	Gimmal Technical Support
Verify that the Gimmal Contract Management Web application log has no errors.	Gimmal Technical Support

A B C D E F G H I J K L M N O P Q R S T U V W

Index