



Administrator's Guide, Part 1:

Design and Configuration

 process backbone

Exigen Workflow 5.6

Process Control Services

Document number: TP_EWF_5.6_Admin_1.7_JO

Revised: 8/9/2005.

EXIGEN CONFIDENTIAL – FOR AUTHORIZED USERS ONLY

Important Notice

Information in this document, as well as the software described in it, is furnished under license and may be used or copied only in accordance with the terms of such license. The content of this manual is furnished for informational use only, is subject to change without notice, may contain technical inaccuracies or typographical errors, and should not be construed as a commitment by Exigen Properties, Inc. and/or affiliates ("Exigen"). Exigen may make improvements and/or changes in the products and/or the programs described in this document at any time without notice. Exigen is not responsible or liable for any changes made to this document without Exigen's prior written consent. In particular, modifications in or to the data model may have occurred or may occur in a new product release after publication of this documentation. In accordance with Exigen standard support policy, any difficulties caused by a modified data model shall not be considered support issues and shall not be covered by Exigen maintenance and support. For further information, consult your support agreement.

Information published by Exigen on the Internet/World Wide Web may contain references or cross-references to Exigen products, programs and services that are not announced or available in your country. Such references do not imply that Exigen intends to announce such products, programs or services in your country. Consult your local Exigen business contact for information regarding the products, programs and services that may be available to you.

In no event will Exigen or its licensors be liable to any party for any direct, indirect, special or other consequential damages for any use of this product or its accompanying publications, including, without limitation, any lost profits, business interruption, loss of programs or other data on your information handling system or otherwise, even if we are expressly advised of the possibility of such damages. Exigen provides this product and its publications "as is" without warranties or conditions of merchantability or fitness for a particular purpose. Some jurisdictions do not allow disclaimer of express or implied warranties in certain transactions; in that case, this notice may not apply.

Copyright

1994-2005, Exigen Properties, Inc. and/or affiliates. All rights reserved.

You may not reproduce this material without the prior express written permission of Exigen Properties, Inc., Legal Department, 505 Montgomery Street, Suite 2300, San Francisco, CA 94111.

Exigen Properties, Inc. and/or affiliates and its licensors retain all ownership rights to this product (including but not limited to software, software libraries, interfaces, source codes, documentation and training materials).

This product's source code is a confidential trade secret. You may not decipher, decompile, develop, or otherwise reverse engineer this software.

Microsoft, Windows, Windows NT, Active Directory, Outlook, Visual Basic, and Win32 are either registered trademarks or trademarks of Microsoft Corporation in the United States and/or other countries.

All other brand names and product names used in this document are trade names, service marks, trademarks or registered trademarks of their respective owners.

This product contains parts of imaging code owned and/or licensed by Pegasus Imaging Corporation, Tampa, FL. All rights reserved.

Parts of this product are developed using FineReader Engine, owned by ABBYY Software House, Fremont, CA. All rights reserved.

Parts of this product are developed using ScanFix Image Optimizer for Windows. Copyright TMS, Inc. All rights reserved.

Contact information

Telephone:

1-866-4EXIGEN	North America
1-800-GoExigen	Europe
61-300-303-100	Australia
1-506-674-6922	All other countries

Ground mail:

Exigen Properties, Inc.
Exigen Support Services
12 Smythe Street, 5th Floor
Saint John, NB, Canada, E2L 5G5

Hours of operation:

Monday through Friday 6:00 a.m. – 9:00 p.m. AST
Outside these hours, on-call 24x7 voicemail is answered within 15 minutes.

Website: <http://www.exigengroup.com/>

Fax: 1-506-674-4014

Email: support@exigengroup.com

Table of Contents

Preface	10
Purpose.....	10
Audience.....	10
Related Information.....	10
Typographic Conventions.....	11
Chapter 1: Introduction	12
What Is Exigen Workflow?.....	12
Workflow Software.....	12
Document Management	12
Document Imaging.....	12
Exigen Workflow Users	13
System Administrators.....	13
End Users	13
Exigen Workflow System Overview	14
Exigen Workflow Data Structure.....	15
Folder, Parcel, and Document Associations.....	15
Working with Folders and Subfolders	15
Working with Parcels	16
Deleting Documents.....	16
Exigen Workflow Administrative Process Overview	16
Exigen Workflow Tools and Utilities.....	17
Exigen Workflow Program Tools	18
Database Tools.....	18
Workflow Tools	18
Servers.....	19
Utilities	19
Servers in Workflows	20
Chapter 2: Getting Started	22
Starting Exigen Workflow	22
Exiting Exigen Workflow.....	24
Exigen Workflow Explorer	24
Chapter 3: Creating Projects.....	27
Overview	27
Project Builder Window	28
Creating a New Project	29
Using a Non-Default Database.....	34
Project Table Maintenance.....	34
Project Table Maintenance Window	35
Adding and Modifying Fields	37
Defining a Field with Create/Modify by Reference	40
Copying Tables.....	47
Managing Views	47
Defining Batch Status Option	54
Setting Internal Counters.....	56
Recreating Project Indexes	57
Exigen Workflow Security.....	57
Role Based Security	58
ACL Based Security.....	59
Setting Up Document Versioning.....	61

Configuring the Project.....	62
Location Tab	63
Indexing Tab	64
QA Tab.....	66
Optical Tab	67
Document Management Tab	69
Email Tab.....	70
E-Forms Tab.....	72
Security Tab.....	73
Copying or Renaming Projects	75
Exporting Projects	77
Exporting Tables	77
Exporting Data	79
Importing Projects	81
Importing Tables	81
Importing Data	83
Checking the Project Version	84
Full Text Search	86
Unique and Cluster Indexes	87
Unique Indexes	87
Cluster Indexes	88
Advanced Features	88
Using an Oracle Database with Synonyms.....	88
Chapter 4: Setting Up Exigen Workflow	90
Overview	90
Setting Up the System.....	92
Specifying Security Settings	95
Specifying Audit and Reconnection Settings.....	97
Defining Audit Filters.....	98
Configuring Document and Page Notes	102
Using the System Setup Window	103
Specifying Security Levels.....	103
Specifying Access Levels	115
Setting Up Workflow Objects	119
Setting Up Workflow Groups	124
Setting Up Corporate Locations	127
Setting Up Users.....	132
Setting Up Tasks	144
Setting Up Events	149
Managing Stamps.....	152
Setting Up Locations.....	154
Setting Up Global User Groups	155
Setting Up Document Context Security Levels.....	161
Setting Up Document Types.....	166
Setting Up Skills.....	170
Setting Up and Using Annotation Security	178
Maintaining Project Tables	182
Maintaining Storage Locations	185
Maintaining Optical Disk Devices	185
Maintaining Image Servers.....	190
Scheduling Activities	193
Scheduled Activities Window.....	197
Activity Window.....	197
Audit Event Cleanup	198
Setting Up Document Access Control	199

Defining Privileges	200
Defining Entitlements	203
Defining Permissions	206
Defining Security Entries	208
Setting Up and Printing Reports	210
Viewing and Modifying Configurations	213
What Is Configuration Browser?	213
Configuration Browser User Interface	214
Using Configuration Browser	217
Managing Configuration Schemas	241
Configuration Browser Menu Commands and Buttons	248
Setting Up Folder History Browsing	250
Creating a Link Navigation Section	251
Specifying Link Navigation Settings	252
Specifying Scanner Specific Settings	254
Chapter 5: Designing a Workflow	255
Overview	255
Main Concepts	256
List of Workflow Objects	257
Main Steps to Creating a Workflow	259
Designing a Workflow Map	259
Using Workflow Builder	260
Setting Up Workflow Objects	263
General Tab	264
Form Tab	269
Rules Tab	272
Send Tab	272
Escalation Tab	273
Monitor Tab	274
E-Forms Tab	275
Taskflow Tab	275
Additional Settings Tab	276
Maintaining Workflow Nodes	277
Setting Up Workflow Links	278
Exigen Workflow Events	282
Modifying Workflows in List Mode	285
Changing Workflow Properties and Access Rights	286
Modifying Nodes and Links	288
Running and Testing a Workflow Object	289
Changing the Node Sort Order	290
Using an Alias	290
Using a Case	292
Creating a Submap	292
Setting Up Workflow Routing Rules	293
Integrating with Exigen E-Forms	298
Using an Oracle Stored Procedure for the Common Queue	301
Creating a Stored Procedure	301
Setting Up a Stored Procedure	302
Simulating a Workflow	303
Using Designer Mode	304
Using the Hidden Mode Feature	304
Setting Viewer Focus	305
Tips for Building a Workflow	306
Exporting and Importing a Workflow	306

Exporting a Workflow	306
Importing a Workflow	308
Managing Components	309
Starting Component Configuration Manager	310
Component Configuration Manager Window	312
Adding a New Component	315
Adding a New Component from a Component	320
Adding an Existing Component from a Component	321
Adding an Inherited Component	321
Removing a Component	322
Exporting Component Configurations	323
Importing Component Configurations	327
Viewing and Modifying a Component	330
Component Configuration Manager Window Buttons and Menu Commands	331
Chapter 6: Managing the Workflow	332
Overview	332
Graphical Queues Workload Monitor Window	333
Graphical Users Workload Monitor Window	334
Workload Distribution Monitor Window	335
Viewing, Distributing, Reassigning, and Printing Parcels	337
Resetting Parcel Times	342
Configuring Node and User Display Settings	343
Deleting Parcels	343
Viewing User Job Statistics	344
Viewing Queue Job Statistics	347
Understanding the Workload Distribution Monitor Window	347
Dealing with Problematic Documents	351
Using Document Versioning	352
Chapter 7: Statistical Analysis	353
Overview	353
Viewing Statistics and Reports	353
Chapter 8: Process Monitor	358
Overview	358
Using Process Monitor	358
Configuring Process Monitor Settings	360
Notifying Users about Stopping a Connection	361
Updating the Connection List	361
Setting the Refresh Frequency	361
Printing the Process Monitor List	361
Sending a Message	361
Disabling Connections	362
Specifying Sort Order	362
Clearing the Process Monitor	362
Saving the Configuration	363
Chapter 9: Setting Up Exigen E-Capture	364
Overview	364
Special Features	365
Introducing E-Capture Administrator	366
Getting Started	366
Selecting a Project	367
Defining Field Types	368
Adding a Field Type	370

Modifying a Field Type.....	371
Deleting a Field Type.....	372
Defining Output Groups.....	372
Adding an Output Group.....	373
Modifying an Output Group	374
Deleting an Output Group.....	375
Defining Output Details.....	375
Registering Vendors.....	381
Adding a Software Vendor.....	381
Modifying a Software Vendor	382
Deleting a Software Vendor.....	383
Defining Policy Types.....	383
Adding a Policy Type.....	385
Modifying a Policy Type.....	385
Deleting a Policy Type.....	386
Defining Form Categories	386
Sequencing Form Categories.....	388
Adding a Form Category.....	388
Modifying a Form Category	389
Deleting a Form Category.....	390
Registering Special Forms	390
Adding a Special Form	392
Modifying a Special Form	393
Deleting a Special Form	393
Separating Documents Based on Bookmarks	394
Overview	394
Restrictions	395
Setting Up the Separation of PDF Files Based on Bookmarks	396
Assigning Diagnoses.....	396
Adding a Diagnosis.....	397
Modifying a Diagnosis.....	398
Deleting a Diagnosis.....	399
Registering Companies	399
Adding a Company	400
Modifying a Company	401
Deleting a Company	402
Using E-Capture Custom Scripts.....	402
Overview	403
Setting Up and Running E-Capture Custom Scripts	403
Script Example.....	404
Registering Scripted Modules.....	405
Registering Scripts.....	411
Chapter 10: Setting Up User Synchronization Service	420
Overview	420
ADSync Functionality	421
Logging Function.....	422
Installing ADSync	423
System Requirements	423
Installation.....	423
Configuring ADSync.....	424
Synchronization with Directory Services	424
Connecting to a Database Using OLE DB.....	426
Configuring ADSync and Mapping a Directory Service	427
Exposing Internal ADSync Objects For Use in Mapping Scripts	434
Mapping Examples	434

Registering and Running the ADSync Module.....	439
Customizing Exigen Workflow	440
Exigen Workflow Audit Events Generated by ADSync.....	440
Setting up Exigen Workflow User Groups, Global User Groups, and Security Levels.....	441
User-Level Security	442
Modifying the Security Level.....	442
Integrating Integrated Security Management Console with ADSync	444
Overview	444
Customizing Exigen Workflow	445
Exigen Security Services Elements Collection Plug-in.....	445
Chapter 11: Using Audit Log Viewer	449
Filtering Audit Records	450
Activating Filters	451
Deactivating Filters	451
Resetting to Initial Current Filters	451
Creating Filters	451
Copying Filters	452
Editing a Filter Definition.....	453
Deleting Filters	453
Customizing Columns and Column Filters.....	453
Setting Column Filters	454
Sorting Audit Records	455
Searching Audit Records.....	455
Exporting Audit Records.....	456
Deleting Audit Records.....	457
Refreshing Audit Records	457
Copying Audit Records.....	457
Archiving Audit Records	457
Audit Archive Filter.....	458
Appendix A: Exigen Workflow Object Menus and Button Bars.....	461
Exigen Workflow Explorer	461
Project Builder	462
Project Table Maintenance.....	464
Appendix B: Default Tables for New Exigen Workflow Projects	467
Appendix C: Using .ini Files for Internationalization and Path Substitution	469
Configuring Internationalization	469
Formatting Dates and Times in the visiclt.ini File	469
Entering Database Server Names in the visi.ini File	471
visi.ini File Database Server Section Examples	472
Path Substitution	474
Overview	474
Enabling Path Substitution	475
Example	475
Appendix D: Audit Data in Exigen Workflow	476
Exigen Workflow Audit Log Data	476
Audit Log Data Groups	476
PROJECT ID_AUDIT_LOG Table.....	478
Audit Configuration.....	480
Audit Algorithm	480
Local Audits	481

Sample Audit Configuration	482
PROJECT ID_AUDIT_MSGID Table.....	483
S23_AUDIT_FILTER Table	484
Audit Event Descriptions.....	485
Audit Server	505
Appendix E: Diagnoses	507
Appendix F: ScriptCalls	508
Appendix G: Exigen Workflow User Authentication Mechanism	510
Authentication Mode.....	510
Database Connection Mode	510
Database Permissions.....	511
Implementing Database Authentication.....	513
Required Privileges for SQL and Oracle Databases	514
Available Configurations for the Authentication and Database Connection Modes	515
Switching between Database Users	515
Multiple Database Servers and Database Authentication	515
Performing a Single Login	516
Performing a Trusted Login	516
Appendix H: How ACL Based Security Affects Documents, Folders, and Subfolders.....	518
Inheriting Security Settings.....	518
Restrictions on Operations with Documents, Folders, Subfolders, and Parcels	518
Glossary	520
Index	534

Preface

The following topics are described in this section:

- [Purpose](#)
- [Audience](#)
- [Related Information](#)
- [Typographic Conventions](#)

Purpose

This guide defines the main concepts underlying Exigen Workflow and describes how to create projects and set up, manage, and monitor the system.

Audience

This guide is intended for system administrators.

This guide assumes basic computer knowledge for performing Windows® operations. It also assumes a familiarity with ODBC and basic experience working with the SQL language and databases.

Related Information

The following table lists guides that provide related information about Exigen Workflow:

Related documentation	
Title	Description
<i>Exigen Workflow User's Guide</i>	Describes how to operate Exigen Workflow.
<i>Exigen Workflow Installation Guide</i>	Describes how to install Exigen Workflow.
<i>Exigen Workflow Administrator's Guide II: Business Component Reference</i>	Describes how to configure and use Exigen Workflow server components.
<i>Exigen Workflow Administrator's Guide III: Utilities</i>	Describes how to use Exigen Workflow utilities.
<i>Exigen Workflow Web User's Guide</i>	Describes how to use the Exigen Workflow Internet solution.
<i>Exigen Workflow Web Administrator's Guide</i>	Describes how to administer the Exigen Workflow Internet solution.

Typographic Conventions

The following styles and conventions are used in Exigen documentation:

Typographic styles and conventions	
Convention	Description
Bold	<ul style="list-style-type: none"> Represents user interface items such as check boxes, command buttons, dialog boxes, drop-down list values, field names, menu commands, menus, option buttons, perspectives, tabs, tooltip labels, tree elements, views, and windows. Represents keys, such as F9 or CTRL+A. Represents a term the first time it is defined.
Courier	Represents file and directory names, code, system messages, and command-line commands.
Courier Bold	Represents emphasized text in code.
Select File > Save As	Represents a command to perform, such as opening the File menu and selecting Save As .
<i>Italic</i>	<ul style="list-style-type: none"> Represents any information to be entered in a field. Represents documentation titles.
< >	Represents placeholder values to be substituted with user specific values.
Hyperlink	Represents a hyperlink. Clicking on this field takes you to the identified place in this guide.

Chapter 1: Introduction

This section introduces the Exigen Workflow system.

The following topics are described in this section:

- [What Is Exigen Workflow?](#)
- [Exigen Workflow Users](#)
- [Exigen Workflow System Overview](#)
- [Exigen Workflow Data Structure](#)
- [Deleting Documents](#)
- [Exigen Workflow Administrative Process Overview](#)
- [Exigen Workflow Tools and Utilities](#)

What Is Exigen Workflow?

Exigen Workflow is a customizable workflow management and document imaging system. Exigen Workflow enables system administrators to create workflow applications for solving document management problems. End users use these applications to scan, import, index, view, route, archive, and retrieve documents.

The following Exigen Workflow software components are described in this section:

- [Workflow Software](#)
- [Document Management](#)
- [Document Imaging](#)

Workflow Software

Workflow software provides structured processing and rules that enable to route imaged and other electronic documents through your organization without additional programming.

Document Management

Document management software provides indexing, handling, storage, and retrieval of imaged and other electronic documents.

Document Imaging

Document imaging software converts paper documents into computerized document images. These document images are viewed and edited as needed.

Scanning converts paper documents, including text, illustrations, and photos, into computer document images. Any document can be scanned into a computer and filed, distributed, or processed. Scanned images can also be printed or faxed.

Exigen Workflow assigns field values to parcels and document images and applies barcode values to document images. Routing rules and events allow you to send document images to other users via email. Once document images are indexed, the documents can be accessed by many users. This eliminates the need for photocopying and interoffice mail.

Exigen Workflow provides security against inappropriate or unauthorized use, improves customer service, increases productivity, and cuts operating costs.

Exigen Workflow Users

The following Exigen Workflow user types are described in this section:

- [System Administrators](#)
- [End Users](#)

System Administrators

System administrators configure and manage the Exigen Workflow system. The following table describes the main setup tasks of the system administrators:

System administrators	
Setup task	Description
Set up user profiles	Establishes permissions and access for end users based on their role within the company.
Customize fields and tables	Customized tables and fields are added to the system and used for indexing and reference material. Custom tables are used as references for certain fields, ensuring that data is entered correctly.
Rule-based routing	Method for guaranteeing that documents are sent to the correct recipients for handling.
Set up tables and workflow	Creates and maintains the tables and workflow.

End Users

End users process documents routed to them with Exigen Workflow. The workflow defines who they can send mail to and who they can receive mail from. Users access specific workflow objects based on their individual user profiles. For example, some users may have access to the Statistical Information Utility, or to the Exigen Workflow Monitor, which allows a parcel to be moved from one queue or user to another.

Exigen Workflow System Overview

Exigen Workflow is a customizable system that enables system administrators to create workflow applications for solving document management problems. End users use these applications to perform the following tasks:

- scan documents
- import documents
- view documents
- route documents
- archive documents
- retrieve documents

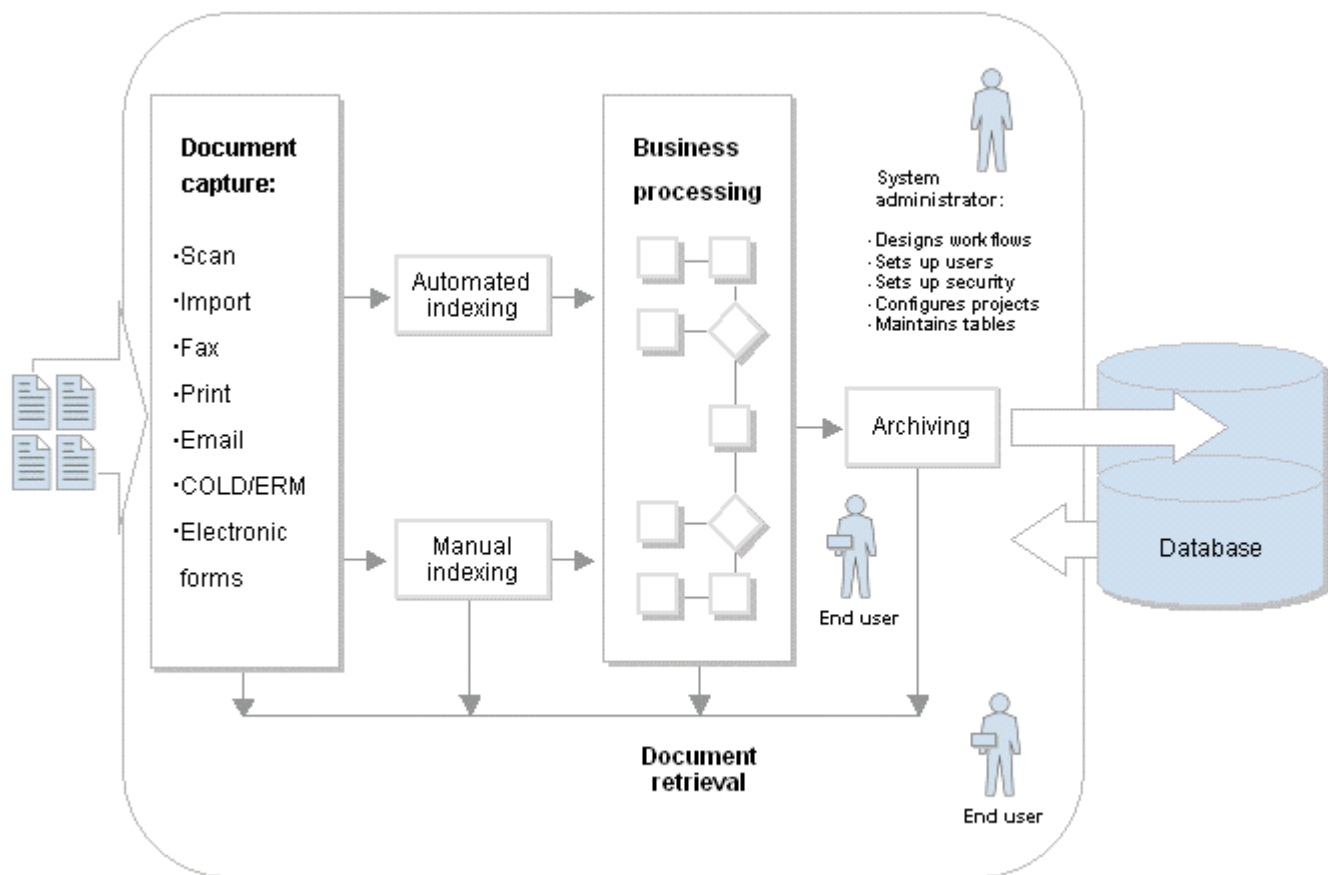


Figure 1: Exigen Workflow system overview

Exigen Workflow Data Structure

The following topics are described in this section:

- [Folder, Parcel, and Document Associations](#)
- [Working with Folders and Subfolders](#)
- [Working with Parcels](#)

Folder, Parcel, and Document Associations

Exigen Workflow works with folders, parcels, and documents. Documents are the most basic objects and are created by scanning paper documents or by using applications such as Word.

Exigen Workflow allows you to store different types of documents in one folder. For example, one folder can have a scanned invoice, a word-processed letter, a spreadsheet file, and a faxed document file.

Documents can be assigned pre-designated names, or document types. Access to specific documents can be restricted per user.

A number system is used to track batches, parcels, documents, and folders in Exigen Workflow.

During the scanning process, a batch number and document number are assigned to the current batch and scanned document. A parcel is also created and given a parcel number. The parcel number is stored in the document's record with the document number.

The following table shows the number structure in Exigen Workflow:

Number structure		
Folder table	Parcel table	Document table
Folder number	Parcel number	Document number
	Folder number	Parcel number
		Folder number

Working with Folders and Subfolders

Folders store related documents. Subfolders represent different sections within a folder. Individual documents are stored in the subfolders.

The following table illustrates how the Exigen Workflow structure is similar to a file cabinet:

Folder and subfolder structure	
In Exigen Workflow	In your file cabinet
Documents	Paper documents
Subfolders	Manila folders
Folders	Hanging folders

By assigning identifying values at the folder, subfolder, and document level, you can organize your electronic file cabinet using the same concepts as the cabinet in your office.

Folders are added dynamically from within the Exigen Workflow indexing application. Assigning unique index fields prohibits the creation of duplicate folders, as Exigen Workflow checks to ensure that the folder does not already exist before it is added.

Subfolders can also be used to index documents. Subfolders are added dynamically or assigned to documents using predefined values. The system administrator configures the indexing system that determines how subfolders are used.

Working with Parcels

Exigen Workflow uses parcels to move documents through the queues in the workflow. Each parcel contains one or several documents, which travel from one workflow node or user to the next. A batch of scanned-in documents can be divided into several parcels depending on their destination. Exigen Workflow assigns a unique Parcel ID number to each parcel. This number is also inserted into the document record for each document contained in the parcel.

During indexing, the parcel is assigned to a specific folder. All documents assigned to that parcel are also indexed to the same folder. If the parcel contains a document that must be indexed to a different folder, the document must be placed into a separate parcel using the available queue tools.

Deleting Documents

In Exigen Workflow, when a document is selected to be deleted by a user or an automated system component, the system does not delete the document immediately but marks the document for deletion and moves it to the recycle bin.

The **recycle bin** is a logical container of Exigen Workflow documents that are marked for deletion. Documents can only be physically removed from the database and document storage systems by Retention Server when it is run in document recycling mode. The process of moving deleted documents to the recycle bin is named **document recycling**. For information on setting up and using Retention Server, see *Exigen Workflow Administrator's Guide, Part II: Business Component Reference*, Chapter 12: Document Retention.

On the database level, when a document is marked for deletion, the document record is moved from the DOCUMENT table to the DOC_RECYCLE table.

By default, document recycling is enabled in all Exigen Workflow applications except Application Services. In Application Services, document recycling must be enabled manually as described in *Exigen Workflow Installation Guide*, Chapter 8: Installing Application Services, Configuring Application Services.

Exigen Workflow Administrative Process Overview

The Exigen Workflow administrative process includes the following tasks:

- project setup
- workflow design, build, and setup
- user and security level setup
- project configuration
- table maintenance

In addition, Exigen Workflow utilities can perform the following functions:

- importing images from other systems
- checking document and database integrity
- monitoring system connections
- processing Enterprise Report Management (ERM)
- generating forms

Exigen Workflow Tools and Utilities

The Exigen Workflow administrator performs the following tasks:


- Exigen Workflow system setup
- configuration
- optical disk management
- system table configuration
- file backup

To make these tasks easier, Exigen Workflow offers the following tools and utilities:



- [Exigen Workflow Program Tools](#)
- [Database Tools](#)
- [Workflow Tools](#)
- [Servers](#)
- [Utilities](#)
- [Servers in Workflows](#)

For a detailed description of Exigen Workflow utilities, see the *Exigen Workflow Administrator's Guide, Part 3: Utilities*.








Exigen Workflow Program Tools





Program tools		
Icon	Tool	Definition
	Exigen Workflow Explorer	Tool like Windows Explorer that uses collapsible folders.

Database Tools



Database tools		
Icon	Tool	Definition
	Project Builder	Creates projects, configures database size, and creates and maintains customized tables, views, and fields. Other functions include defining the indexing scope and location of scanned images as described in Chapter 3: Creating Projects .
	SQL Talk	Used to make independent SQL requests to the database. This tool is used only if you are experiencing problems with the database. For more information on SQL Talk, see <i>Centura SQL Talk for Windows</i> documentation.

Workflow Tools

Workflow tools		
Icon	Tool	Definition
	Administrator	Maintains user profiles, levels, groups, events, tasks, stamp management, and folder and subfolder security. Project configuration and table maintenance are also performed using this application as described in Chapter 4: Setting Up Exigen Workflow .
	Process Monitor	Maintains connections to workflow applications within the Exigen Workflow system. This tool can also be used to terminate hung processes as described in Chapter 8: Process Monitor .
	Statistics	Monitors the workload processed by a specific user on any given day as described in Chapter 7: Statistical Analysis .
	Workflow Builder	Builds and maintains workflow maps. Workflow maps include workflow objects, links, routing rules, user groups, tasks, host applications, and events as described in Chapter 5: Designing a Workflow .
	Workflow Monitor	Monitors the workload currently in the user queues. Work can be redistributed if required as described in Chapter 6: Managing the Workflow .
	Workflow Viewer	Displays the workflow map in read-only mode.
	E-Capture Administrator	Provides the customized environment for E-Capture Definition Utility and E-Capture Server as described in Chapter 9: Setting Up Exigen E-Capture .





Workflow tools		
Icon	Tool	Definition
	Users Synchronization Setup	Used to configure the Active Directory Synchronization Service (ADSync) and set up log level, security level, timeout, default password, and notifications as described in Chapter 10: Setting Up User Synchronization Service . Note: This tool is available only if ADSync is installed.
	Audit Viewer	Displays, sorts, and filters audit records as described in Chapter 11: Using Audit Log Viewer .
	Configuration Browser	Manages configurations of Exigen Workflow components as described in Viewing and Modifying Configurations .
	Component Configuration Manager	Creates and manages reusable workflow components such as plugins, applications, and nodes, which can be inherited by other components as described in Managing Components .







Servers

Servers		
Icon	Server	Definition
	Print Monitor	Manages jobs in the print queue as described in the <i>Exigen Workflow Administrator's Guide, Part 2: Business Component Reference</i> .
	Print Server	Used with printers shared by many users to assist in scheduling the print jobs. Departmental printers are recommended for large print jobs as local desktop printers print images at a much slower rate. This tool is described in the <i>Exigen Workflow Administrator's Guide, Part 2: Business Component Reference</i> .

Utilities







All utilities are described in the *Exigen Workflow Administrator's Guide, Part 3: Utilities*.












Utilities		
Icon	Utility	Definition
	Check Document Utility	Checks for the integrity of the images in the system. Corrupt images can be sent to a queue for special handling.
	Clear Cache Utility	Clears specific cache directories filled during the commit process.
	Empty Folders Maintenance Utility	Creates a file listing all folders to which no documents are assigned. The administrator can delete the empty folders to free up space in the database.
	FTS Maintenance	Configures FTS settings in projects. It defines stopwords and the algorithm for splitting extracted text into words, and detects documents that are not correctly processed.

Utilities		
Icon	Utility	Definition
	Orphan Utility	Locates discrepancies between the database and the actual files.
	Stamp Management	Creates electronic rubber stamps and applies them to the document images.
	Template Management Utility	Creates and maintains form templates for processing Form Overlay and Form OCR (Optical Character Recognition).
	Transfer Utility	Transfers images from Exigen Workflow to other systems.
	E-Capture Definition Utility	Prepares form templates for recognition and data extraction.
	Publisher Packager	Packages data collections together with the Exigen Workflow system files into one directory, which can be written onto a CD.

Servers in Workflows

Administrators configure and run several Exigen Workflow servers. All servers are described in the *Exigen Workflow Administrator's Guide, Part 2: Business Component Reference*.

Servers in workflows		
Icon	Server	Definition
	Barcode Server	Reads bar codes in documents being scanned. The server converts the values into commands that create parcels for the documents and populate the document index fields.
	Form OCR Server	Extracts OCR data from incoming documents based on templates.
	Form OCR QA	Checks and corrects the data extracted during the Form OCR process.
	Form Index Server	Populates the database with data extracted during the Form OCR process.
	FTS (Full Text Search) Preprocessor	Extracts text from each page of every document sent through the workflow. It performs Optical Character Recognition (OCR) on images and uses other methods for other file formats, including DOC, PPT, XLS, and PDF. Custom Conversion Engine plugins can be developed for specific formats. Document search and retrieval can be performed based on the document text.
	FTS (Full Text Search) Server	Creates an index for the FTS. Document search and retrieval can be performed based on the index.

Servers in workflows		
Icon	Server	Definition
	Image Enhancement Server	Improves scanned image quality. The same enhancements are available during the scanning process. The number of enhancements configured in the scanning process directly corresponds to the amount of time it takes to perform the scanning. Using Image Enhancement Server decreases scanning time while ensuring image integrity.
	Import Server	Can import documents into the Exigen Workflow repository without scanning and index the imported documents. The imported documents can be in different formats, including Exigen Workflow DMS, DOC, TXT, PDF, HTML, GIF, and JPEG.
	Distribution Server	Exports imaged files and database records from one database to another.
	Escalation Server	Routes work items and email to escalation-enabled users and queues.
	Push Server	Automatically sends work items to the next node and user according to workflow rules.
	ERM (Exigen Report Management) Setup	Registers the text files, models, and templates that are processed into ERM, Form Overlay, or COLD format via the ERM Indexer.
	ERM Indexer	Used with the ERM Setup object to process ERM and Forms Overlay data. The server extracts data from specified text files based on their file structure and their indexing assignments in the Setup object.
	ERM Storage Maintenance	Used to move ERM storage files from the original location to any other location on the network, including optical storage.
	Report Definition Wizard	Creates templates for extracting data from computer output to laser disk (COLD) reports.
	E-Capture Server	Captures indexing and other information from files in PDF and PCL format and places these files in a workflow.
	Retention Server	Manages the disposal of outdated documents and other documents that are marked for deletion.
	Taskflow Server	Processes tasks and automatically sends parcels to the next workflow node when all required tasks are completed in taskflow nodes.

Chapter 2: Getting Started

The following topics are described in this section:

- [Starting Exigen Workflow](#)
- [Exiting Exigen Workflow](#)
- [Exigen Workflow Explorer](#)

Starting Exigen Workflow

To start Exigen Workflow, select **Start > Programs > Exigen Solution > Exigen Workflow > Workflow Explorer**.

The **Welcome to Exigen Workflow** window appears.

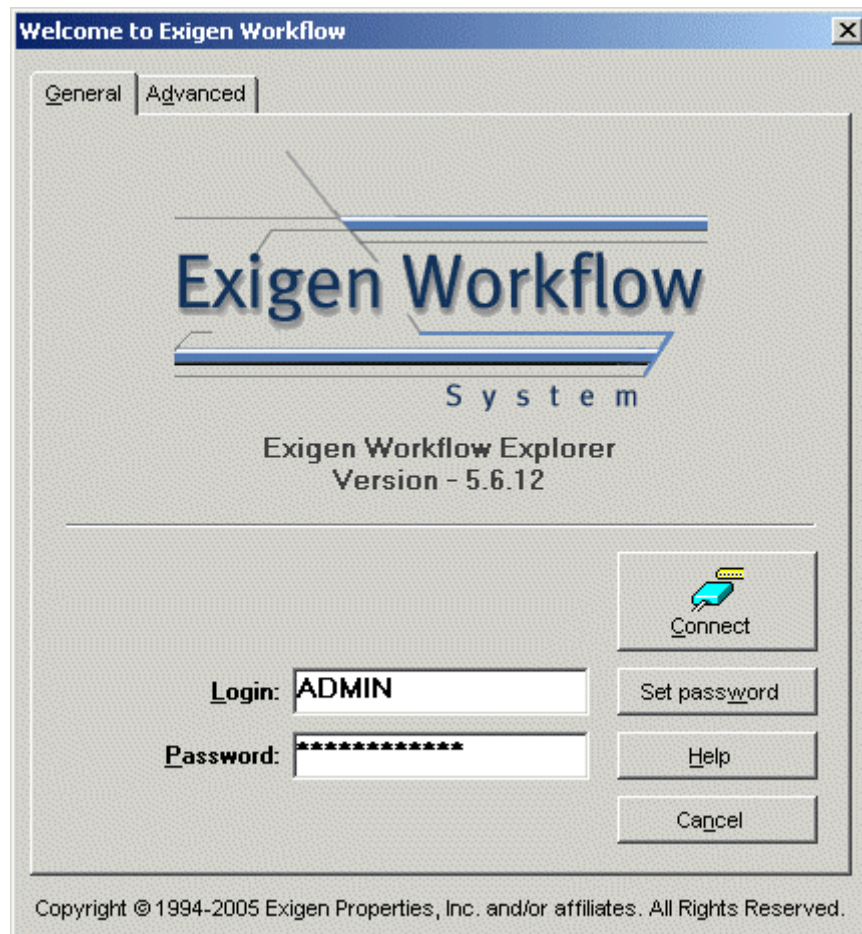


Figure 2: Welcome to Exigen Workflow window

To log in, proceed as follows:

1. In the **General** tab, in the **Login** field, enter the login ID.

The login defaults to capital letters.

2. In the **Password** field, enter your password.

Asterisks mask your password.

Note: Passwords that are not hashed are processed by the security system in a specific way. If the password does not match, the system converts the password to uppercase and tries to validate the uppercase password again. For information on hashing, see [Specifying Security Settings](#).

Note: By default, the same user ID and password can be used to run simultaneous Exigen Workflow sessions at different workstations. For information on prohibiting multiple logins, see [Specifying Security Settings](#).

3. To change your password, click **Set Password**.

The **Change password** window appears.



Figure 3: Change password window

4. In the **New password** and **Confirm new password** fields, enter the new password.
5. To save the new password, click **OK**.

Warning: Immediately change the Exigen default password to prevent any unauthorized logins.

The **Advanced** tab has an additional **Server** field. If you use the Exigen Workflow system with several database servers, this field allows you to connect to more than one server.

To specify connections to multiple servers, proceed as follows:

1. In the **Server** field, select a server in the list.

Note that you can be logged in to multiple servers at the same time.

2. To complete the login process, click **Connect**.

Exigen Workflow Explorer appears, listing all available workflow applications and nodes.

Exiting Exigen Workflow

To exit Exigen Workflow, use either of the following methods:

- Click **Exit** .
- Select **File > Exit**.

Exigen Workflow Explorer

Exigen Workflow Explorer lists all applications, tools, servers, and utilities that the administrator can access. The greeting at the top of the window shows your user ID, your workstation ID, and the current time.

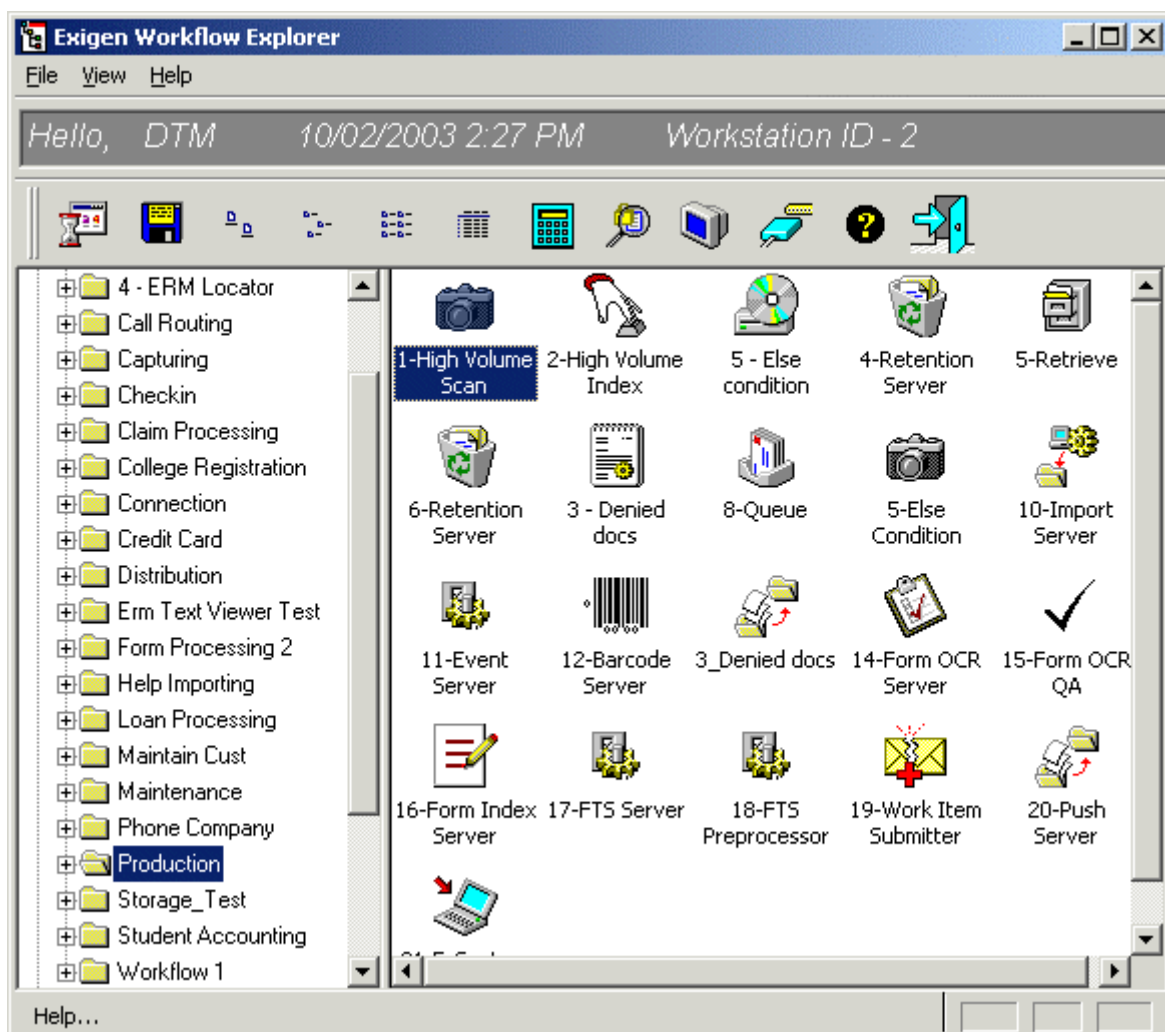


Figure 4: Exigen Workflow Explorer window

For a description of Exigen Workflow menus and toolbars, see [Appendix A: Exigen Workflow Object Menus and Button Bars](#).

To open a workflow object or application, perform one of the following steps:

- Double click on the selection.
- Select it and select **File > Open Application**.
- Right click on the selection and select **Open**.

Expanding the **Applications** folder reveals additional folders that represent different workflow applications. All workflow applications to which you have access are listed. Expanding a workflow application folder reveals an application's workflow objects. The system administrator assigns users access to specific applications and workflow objects.

Expanding the **Administration Tools** folder reveals additional folders that represent the tools and utilities to which you have access. Regular users do not have access to these tools. Administration tools are grouped by their functionality as follows:

Administration tools	
Tool set	Description
Database Tools	Design and maintain the Exigen Workflow projects and databases.
Workflow Tools	Create and maintain workflows, monitor and analyze workflow jobs, maintain user profiles, and monitor system login activity.
Servers	Print from the print queues.
Utilities	Maintain and manage additional administrative aspects of the Exigen Workflow system. For more information about utilities, see the <i>Exigen Workflow Administrator's Guide, Part 3: Utilities</i> .

To change workstation settings, proceed as follows:

1. In Exigen Workflow Explorer, select **File > Workstation Setup**.

The **Workstation Setup** window appears.

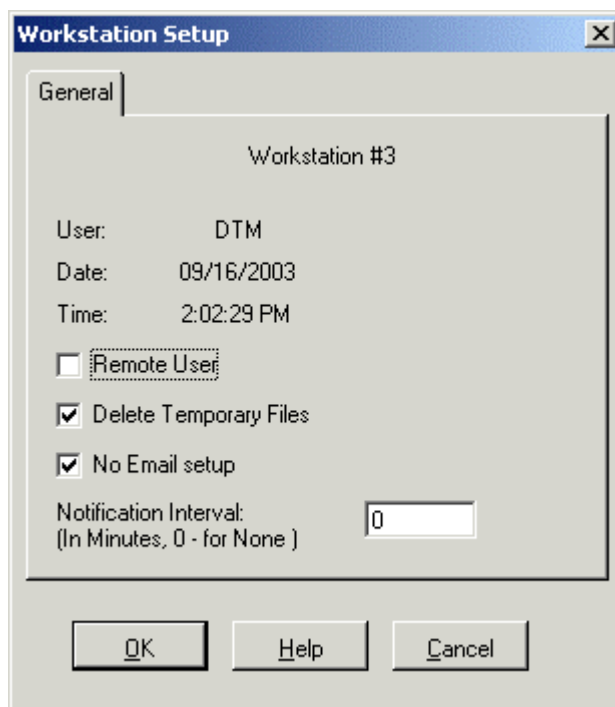


Figure 5: Workstation Setup window

2. In the **General** tab, configure settings as described in the following table:

Workstation setup	
Setting	Description
Remote User	Selected if the current user is connecting to the Exigen Workflow system through a network. Retrieval of DMS images is configured so that only a low-resolution image is initially retrieved. If the image is zoomed, the complete image is downloaded. When using this configuration, the required bandwidth to view an image is reduced.
Delete Temporary Files	If selected, Exigen Workflow automatically removes temporary files when they are no longer required.
No Email setup	If cleared, the user can receive email notifications. If selected, the user cannot use some Exigen Workflow features, such as email notification, during the escalation process.
Notification Interval	Defines the time, in minutes, after which a user is notified about new parcels in the user's queue. Users are not notified about parcels that are distributed using Workflow Monitor or are merged into an existing parcel. If 0 is entered, no notifications are sent.

3. To save changes and close the window, click **OK**.

Chapter 3: Creating Projects

This chapter describes how to customize Exigen Workflow and set up the storage structure and information retrieval.

The following topics are described in this section:

- [Overview](#)
- [Project Builder Window](#)
- [Creating a New Project](#)
- [Using a Non-Default Database](#)
- [Project Table Maintenance](#)
- [Exigen Workflow Security](#)
- [Setting Up Document Versioning](#)
- [Configuring the Project](#)
- [Copying or Renaming Projects](#)
- [Exporting Projects](#)
- [Importing Projects](#)
- [Checking the Project Version](#)
- [Full Text Search](#)
- [Unique and Cluster Indexes](#)
- [Advanced Features](#)
- [Using an Oracle Database with Synonyms](#)

Overview

The purpose of Exigen Workflow is to automate document and task processing. Documents travel through a company in a series of steps from one employee to another until the document is archived. The same process applies to electronic documents in the Exigen Workflow system, but they are not printed and handed from one employee to another. The documents are stored in a database and employees can access those documents addressed to them at any time.

Each database only holds related documents grouped by subject. For example, personnel management or customer invoices. In Exigen Workflow, each subject database is named a **project**.

Indexing structures separate one project from another. For example, in a Personnel Management Project documents might be indexed by Social Security Number (SSN) and Employee Name, whereas in an Invoice Processing Project documents might be indexed by Invoice Number and Dollar Amount. This difference in the indexing scheme requires the creation of two projects. Using the **Project Builder**, the system administrator creates these new projects and sets up the indexing schemes.

The **Project Builder** tool is used to perform the following tasks:

- set up and maintain database table and view structures
- scan directory assignment
- index criteria and database size within each project
- define project attributes, such as Full Text Search
- create and drop unique and clustered indexes
- ensure that new releases of Exigen Workflow are in sync with existing database structures

Project Builder Window

Once Exigen Workflow is installed, the administrator creates a project that stores all information about documents in the company workflow.

To open the Project Builder application, proceed as follows:

1. In Exigen Workflow Explorer, select **Administration Tools > Database Tools**.
2. Double click the **Project Builder** icon.



The main **Project Builder** window appears.

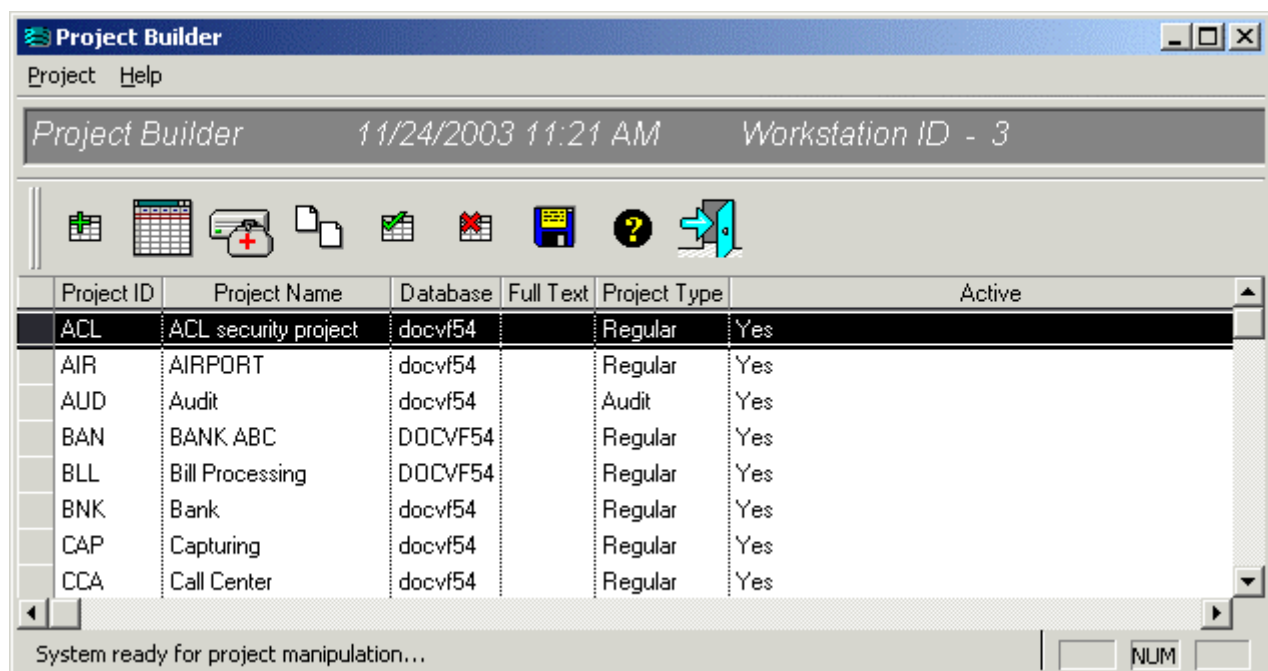


Figure 6: Project Builder window

For information on buttons and menus available in **Project Builder**, see [Project Builder](#). Buttons and menus are described in this section.

Creating a New Project

To create a new project, proceed as follows:

1. In the **Project Builder** window, click **New**.

The **Create New Project** window appears.

Figure 7: Create New Project window

2. In the **Project ID** field, enter a three-character project ID.

The first character must be a letter, while the other two are alphanumeric. This ID is used as follows:

- define which tables belong to each project
- define the scan directory for images scanned into this project
- identify which workflow applications use the tables in this project

3. In the **Project Type** list box, select one of the following project types:

Project types	
Type	Description
Regular	Creates a normal project, which can be attached to standard workflow applications.

Project types	
Type	Description
Storage	Creates a project that allows creating workflows only with the following three workflow objects: <ul style="list-style-type: none"> • ERM Indexer • ERM Setup • ERM Storage Maintenance
Audit	Creates a project for storing audit data. For more information on audit projects, see Appendix D: Audit Data in Exigen Workflow .

Note: Audit projects are used only for storing audit data. They cannot be used instead of regular projects and cannot be associated with the user-defined workflow.

4. In the **Project Name** field, enter the name of the project, for example, *Invoice Processing*.

The project name can have both with uppercase and lowercase letters and can be up to 20 alphanumeric characters long.

5. In the **Database** field, select the name of the project's database, or to automatically enter the default database name, click **Default** to automatically enter the default database name.

For information on using a non-default database, see [Using a Non-Default Database](#).

6. If you use extended security and are creating a project in a database that is not the default database, proceed as follows:
 1. Create a database user for that database with the same name and password as the user of the default database.
 2. Assign the user administrative rights as described in [Database Permissions](#).
7. To test your database connection, click **Connect**.

Note: You can use different database names within the same Exigen Workflow system. The default name is specified during Exigen Workflow installation.

If you create the project in an Oracle, DB2 z/OS, or DB2 AIX database, the **Tablespace** drop-down list box appears after clicking **Connect**.

8. Select one of the tablespaces created for your database.
9. To open the **Space Calculation** window, click **Next**.

The **Space Calculation** window appears.

Space Calculation

Correct the default setting for counters (if needed) and click Calculate Database Size.

	Table Name	Length of Standard Records	Total Number of Fields	Length of Standard Indexes	Total Index Fields	Length of Additional Fields	Length of Additional Indexes	Maximum Number of Records	Required Table Space	Required Index Space
→	FOLDER	8	2	12	3	100	30	30000		
→	SUBFOLDER	12	3	20	5	0	0	100		
→	DOCUMENT	1724	39	53	7	0	0	150000		
→	BATCHPARCEL	602	24	52	6	0	0	5000		


 Set to Default Help Cancel

Figure 8: Space Calculation window

The **Space Calculation** window displays the standard attributes for the four core tables in Exigen Workflow. Information that cannot be edited appears in black. The core tables are described in the following table:

Core tables description	
Table	Description
Folder	Stores the highest level of index information. It tracks all folders in a project. The Folder table is comparable to a hanging file folder in a file cabinet.
Subfolder	Stores the next level of index information. Groups of related documents can be indexed in subfolders, making it easier to search for specific documents. The Subfolder table is comparable to a manila file folder, which resides in a hanging file folder in a file cabinet.
Document	Stores document records. When indexing documents, each document record is assigned the values of the Folder and Subfolder tables, allowing you to quickly search and retrieve a document at any index level. The Document table is comparable to a document stored in a manila file folder, which resides in a hanging file folder in a file cabinet.
Batchparcel	Stores batch and parcel records. A batch is a group of documents scanned into the system together. A parcel is a container for one or more documents and is used to route documents through the workflow. Once documents are sent to an optical medium, the corresponding Batchparcel record can and must be deleted. A Batchparcel record is comparable to an envelope that is used for document delivery.

Exigen Workflow allows you to create custom fields and tables. The space you use for custom fields is shown in the following columns:

- **Length of Additional Fields**
- **Length of Additional Indexes**
- **Maximum Number of Records**

These columns show the default values.

10. Change the default values to correspond to the number of custom fields you intend to add.

For example, each folder in your system represents one client. In addition to the default fields, you require the following four fields:

Required fields	
Name	Length
Client ID Number	10
Client Name	30
Client Phone Number	10
Client Address	50

The fields have a total length of 100 characters. For this example, the following values are appropriate:

- In the **Length of Additional Fields** column, enter 100.
- Because the **Client ID Number** and **Client Name** are the only custom fields that can be used for indexing, in the **Length of Additional Indexes** column, enter 40.
- If you have a maximum of 50,000 customers, you have 50,000 folder records. In the **Maximum Number of Records** column, enter 50,000.
- If you expect to receive no more than 10 documents from each of your customers, in the **Document** row of the **Maximum Number of Records** column, enter 500,000.

11. After entering all the required values, click **Calculate Database Size**.

The **Required Table Space** and **Required Index Space** are calculated and displayed in kilobytes (KB) in the corresponding columns. The **overall space necessary for the project** appears in the top part of the window.

12. Make sure that the database size shown in the **Required Space** field corresponds to the actual space you have on your server.

Note: The Space Calculator does not allocate space. It calculates approximately how much free database space in KB is required on the server. The numbers specified in the Space Calculator do not restrict the actual space you can use for fields or records.

Space Calculation

Required Space (KB): **409396**

There are no problems detected: click 'Create New Project' to continue.

	Table Name	Length of Standard Records	Total Number of Fields	Length of Standard Indexes	Total Index Fields	Length of Additional Fields	Length of Additional Indexes	Maximum Number of Records	Required Table Space	Required Index Space
→	FOLDER	8	2	12	3	100	30	30000	4047	1985
→	SUBFOLDER	12	3	20	5	0	0	100	7	9
→	DOCUMENT	1724	39	53	7	0	0	150000	310786	12763
→	BATCHPARCEL	602	24	52	6	0	0	5000	3702	417





Set to Default
Help
Cancel

Figure 9: Calculated table space

13. When the required table and index space in the **Space Calculation** window is appropriate, click **Create New Project**, which appears to the right of the **Calculate** button after the required space values are calculated.

The **Create Database Structure** window appears and the system creates required system tables, indices, and columns. When the process is complete, a project record appears in the **Project Builder** window.

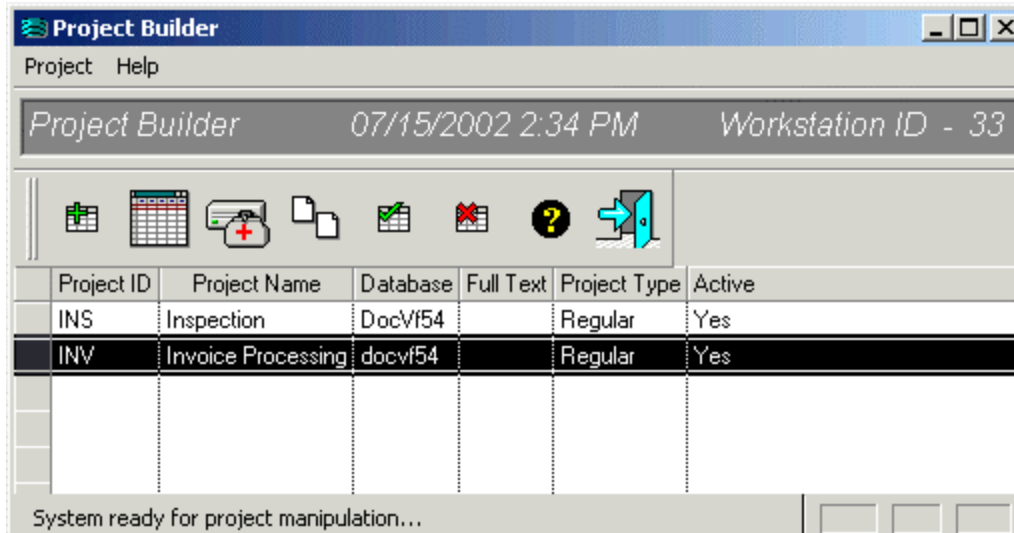


Figure 10: Project Builder window with the created project

The next step is to define index fields and add custom fields or tables.

Using a Non-Default Database

When creating, copying, or importing a project using a non-default database, consider the following factors:

- Project Builder automatically runs the required scripts. However, if you upgrade Exigen Workflow, you must update the master database using Workflow DB Startup as described in the *Exigen Workflow Installation Guide*, Chapter 2: Installing Exigen Workflow.
- It is not necessary to run Workflow DB Startup on the non-default database. To update projects, use the Check Project Version feature as described in [Checking the Project Version](#).

Note: Do not run the Check Project Version feature using a previous release of Exigen Workflow on a project created with a newer release.

- Database server versions can differ, but the brand must be the same. For example, SQL and Oracle database servers cannot be used together.
- If the non-default database is located on a DB2 database server, a specific entry must be manually added in the `visi.ini` file for the database as described in *Exigen Workflow Installation Guide*, Chapter 3: Setting Up the Database Connection.

Project Table Maintenance

To see all tables for a specific project, double click the project name or ID in the **Project Builder** window. The **Project Table Maintenance** window appears, listing all table names associated with the project. Each table name is preceded by the Project ID and an underscore. For example, if your project

ID is INV, a possible table name is INV_BARCOLUMN. For information on Exigen Workflow default tables, see [Appendix B: Default Tables for New Exigen Workflow Projects](#).

When a new project is started, Exigen Workflow loads all tables and fields required to run Exigen Workflow. Adding new tables and fields can customize the project's table structure.

The following topics are described in this section:

- [Project Table Maintenance Window](#)
- [Adding and Modifying Fields](#)
- [Defining a Field with Create/Modify by Reference](#)
- [Copying Tables](#)
- [Managing Views](#)
- [Defining Batch Status Option](#)
- [Setting Internal Counters](#)
- [Recreating Project Indexes](#)

Project Table Maintenance Window

To open the **Project Table Maintenance** window, select the project you want to work with and click **Project Maintenance** or double click the project. The **Project Table Maintenance** window appears.

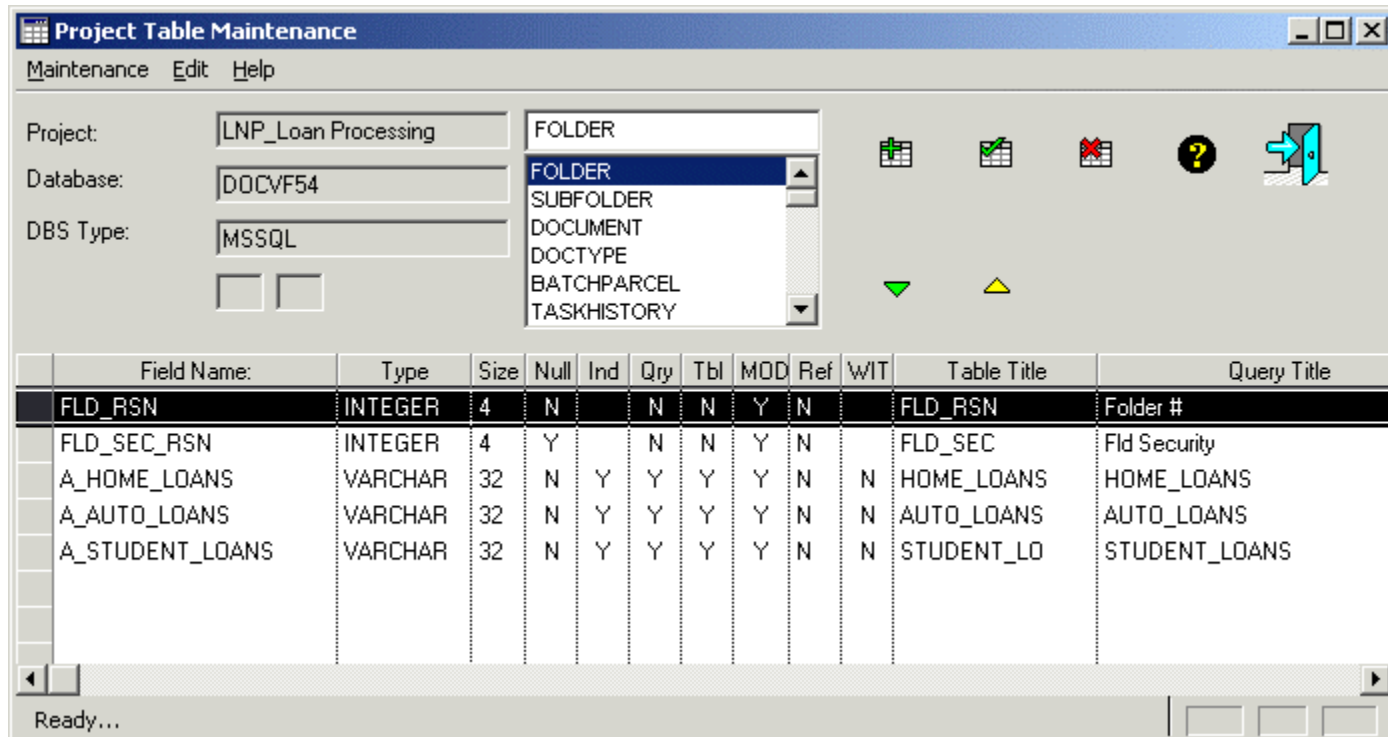




Figure 11: Project Table Maintenance window

The window shows **Project** and **Database** identification attributes, a list of existing tables in the project, and a detailed list of the fields and their attributes for the selected table.

The **Project Table Maintenance** window includes the following data fields:

Project Table Maintenance window, data fields	
Data field	Description
Project	Project name preceded by the project ID and an underscore.
Database	Database to which the project is assigned.
DBS Type	Database server type to which the project is assigned.
	If displayed, unique indexes are created.
	If displayed, Full Text Search tables are created for the project.

In the list box, select a table to manage.

The following table columns are displayed:

Project Table Maintenance window, table columns	
Column	Description
Field Name	<p>Field name.</p> <p>When custom fields are added to a table, the value A_ is inserted automatically before the name.</p> <p>The following restrictions apply to field names:</p> <ul style="list-style-type: none"> • The maximum length is 16 characters, including A_. • Spaces are not allowed. • Underscores must be used to represent spaces between words. • The first character cannot be a number.
Type	<p>Field type as follows:</p> <ul style="list-style-type: none"> • CHAR: character field • VARCHAR: variable character field • INTEGER: numeric field for whole numbers between -2147483648 and 2147483647 • SMALLINT: numeric field for whole numbers between -32767 and 32767 • FLOAT: numeric field that allows decimal points • DATE: date field • TIME: time field • DATETIME: date and time field
Size	Displays the field length. Note that you can only change the field length for field types of CHAR and VARCHAR. All other types have a pre-assigned length.
Null	<p>Null not allowed.</p> <p>If Y, this field requires a value. If N, the field is optional. Note that records are created once scanning begins. Therefore, Y assigned to a field on any table other than the Folder table requires a value to be entered at the time of scanning. Since folders are created during indexing, a Null Not Allowed setting ensures that all required values must be entered.</p>

Project Table Maintenance window, table columns	
Column	Description
Ind	<p>Part of the Unique Index.</p> <p>If Y, this field performs the following two functions:</p> <ul style="list-style-type: none"> creates a unique index for the combination of fields that have Y as their values correctly updates and inserts records <p>For example, if you are creating a project for an Accounting application, you can use Vendor Number, Vendor Name, and Fiscal Year as your Folder fields. If you only assign the Vendor Number field to part of the unique index, each time a document comes in and is assigned the same number, it is indexed to the same folder regardless of the Vendor Name or Fiscal Year. If you make both the Vendor Number and Fiscal Year part of the unique index, the documents is assigned to a folder based on the unique combination of values in those fields. If multiple Vendor Names documents are to be assigned to different folders, make that field part of the unique index to include it in the unique combination.</p> <p>The first function applies to the Create Unique Index function.</p> <p>Warning: FOLDER and SUBFOLDER tables must contain at least one index field, which is not created automatically. It must be added manually.</p>
Qry	Appears in the Query window. If a table is defined as appearing in the Query window, an index is automatically created to expedite searches.
Tbl	Appears in the Table window.
MOD	Appears in the Modify window.
Ref	Values for this field are selected as records from another table.
WIT	<p>Word in Text. This feature is available only for FOLDER level fields.</p> <p>If Y, this field performs searches for specific words assigned as index values, as it recognizes separate words inside a string.</p> <p>For example, if you are using A_ADDRESS_1 as a field in your table, and during indexing you enter the value <i>1100 Main St., Suite 300</i>, you can later perform a query on the A_ADDRESS_1 field using any portion of the value entered. Without Word In Text, the search is limited to the exact string or <i>1100</i> followed by wildcards.</p> <p>Note: Word in Text uses a single word as its search value. If two or more words are entered, they are treated as one long word. Because this long word is not present in the index, the search is unsuccessful.</p>
Table Title	Displays the title that appears in the Table window for the field. The table title can be up to 10 characters long.
Query Title	Displays the title that appears in the Query window for the field. The query title can be up to 30 characters long.

Note: If a view is assigned to the table, the fields appear in the **Qry**, **Tbl**, and **MOD** windows according to rules set in the view.

Adding and Modifying Fields

To add a field in a table, proceed as follows:

1. In the list box, select the table.

- To open the **Add New Field** window, click **New Field**.

The **Add New Field** window appears.

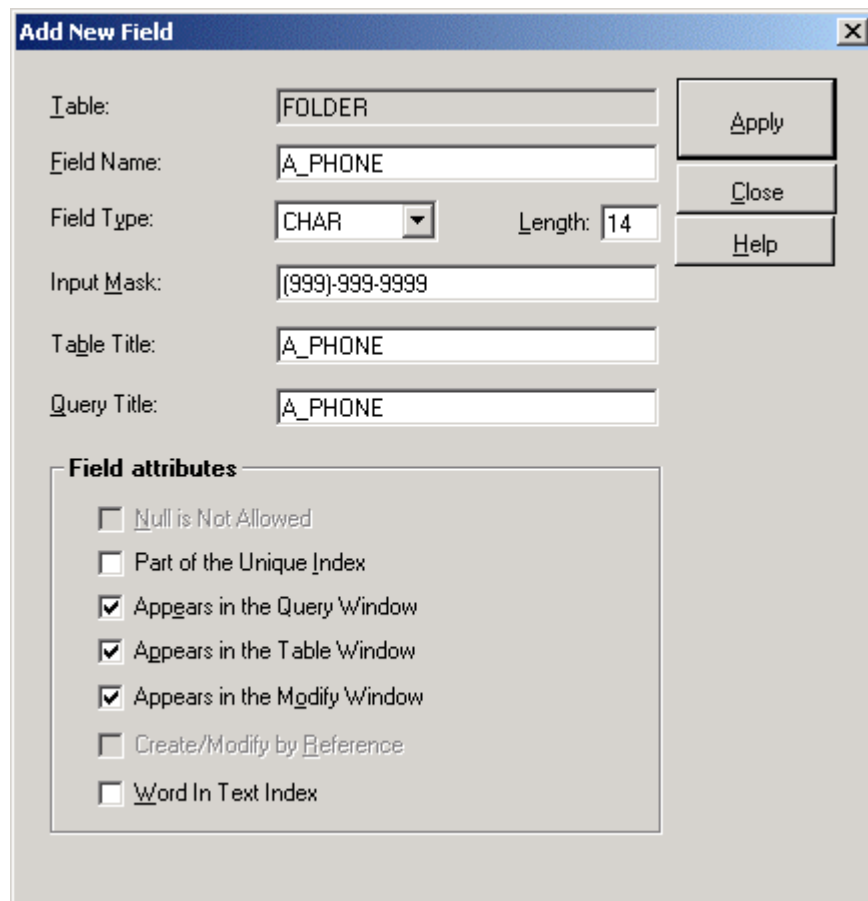


Figure 12: Add New Field window

The table name is displayed in the **Table** field.

- Enter appropriate data in the following fields:

- **Field Name**
- **Field Type**
- **Length**, if CHAR or VARCHAR type
- **Table Title**
- **Query Title**

Note: Floating number fields can contain up to 16 symbols including the sign and comma and not including trailing zeroes after commas.

- To create a mask, in the **Input Mask** field, enter appropriate values.

For example, if the field is a social security number (SSN), you can enter the mask 999-99-9999. When a user enters a social security number in the field, the dashes automatically appear in the window. Any characters included in the mask must be included in the total character length. The SSN example requires a total character length of 11.

The mask sets the maximum length for the user's input. It can be shorter than the mask. For example, if the mask is 9999-999, the user's input can be either 1234 or 1234-123.

Note: The input mask is available only if the length of the **CHAR** or **VARCHAR** field does not exceed 60 characters.

The following table shows the special symbols used to compose an input mask:

Special symbols in input mask	
Symbol	Description
!	Any character, uppercase.
X	Any character.
a	Alpha characters.
A	Alpha characters, uppercase.
9	Digits, 0 through 9.
n	Alphanumeric characters.
N	Alphanumeric characters, uppercase.

A mask cannot be created for a reference field. Do not change input masks when there are existing values.

- Under the **Field Attributes** heading, check the boxes that apply to the new field.

If you do not select the **Appears in Query Window** or **Appears in Table Window** boxes, you do not need to enter values in the corresponding title fields.

- If you want a field to be included in the indexing process, select the **Part of the Unique Index** check box.

Note: FOLDER and SUBFOLDER tables must contain at least one index field, which you must create manually. An index field allows you to use the Index queue in your workflow and to ensure that records are not duplicated.

For information on the **Create/Modify by Reference** check box, see [Defining a Field with Create/Modify by Reference](#). If the field has a mask defined, the **Create/Modify by Reference** check box is disabled.

- To enable a search for specific words assigned as index values, select the **Word in Text** check box.

Note: The **Word in Text** check box can be disabled for some tables because this feature is available only for FOLDER level fields.

- When all required values are entered, click **Apply**.

The field is added to the table but the window remains open, thereby allowing another field to be entered.

- To modify any field, select it and click **Modify Field**, or double click the field entry.

When modifying a field, the field name, field type, length, and **Null is Not Allowed** flag cannot be changed.

10. To delete a field, select it and click **Delete Field**.

Note: Your database might not let you delete fields. In this case, do not add fields unless they are necessary.

11. To rearrange the fields in the **Project Maintenance** window's list, click **Up** and **Down**. Move common fields to the top of the list and less common fields to the end.

The order in which the fields appear in this list is the order they appear in the **Table** and **Query** windows. Moving custom fields above the default fields is not recommended. You can change existing fields to appear in the **Query** or **Table** window if desired.

Defining a Field with Create/Modify by Reference

The **Create/Modify by Reference** function allows you to define a field and a table as a reference table for the selected field. This ensures that only those values that exist in the reference table are entered in the new field. For example, when entering a customer's address, only U.S. states can be used in the corresponding field.

The screenshot shows the 'Add New Field' dialog box with the following fields and options:

- Table:** FOLDER
- Field Name:** A_STATE
- Field Type:** VARCHAR (dropdown menu)
- Length:** 2
- Input Mask:** (empty field)
- Table Title:** A_STATE
- Query Title:** State
- Buttons:** Apply, Close, Help, Values
- Field attributes:**
 - ☐ Null is Not Allowed
 - ☐ Part of the Unique Index
 - ☒ Appears in the Query Window
 - ☒ Appears in the Table Window
 - ☒ Appears in the Modify Window
 - ☒ Create/Modify by Reference
 - ☐ Word In Text Index
- Status bar:** Adding a new field...

Figure 13: Create/Modify by Reference option

To view a list of all tables in the project in the **List of Reference Tables** window, select **Create/Modify by Reference**.

Note: The **Create/Modify by Reference** option can be enabled only for custom fields.

The **List of Reference Tables** window appears.

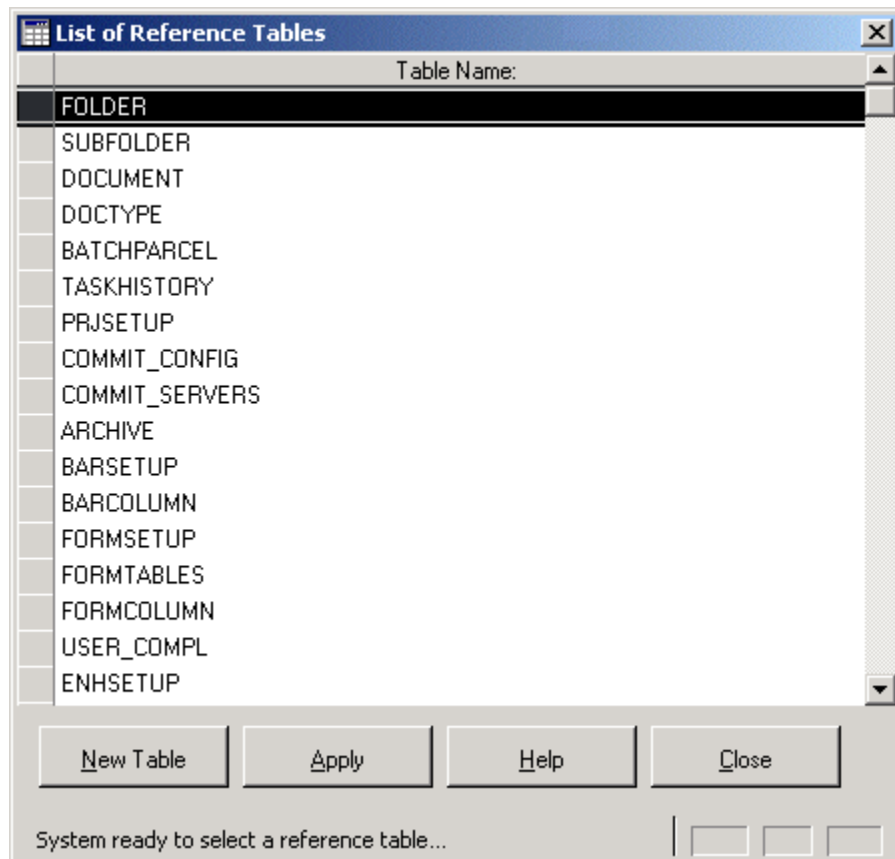


Figure 14: List of Reference Tables window

This section describes how to base a reference table on a new table using the following procedures:

- [Creating a Table](#)
- [Specifying Table Settings](#)

Creating a Table

To create a table, proceed as follows:

1. Click **New Table**.

The **Add New Reference Table** window appears.

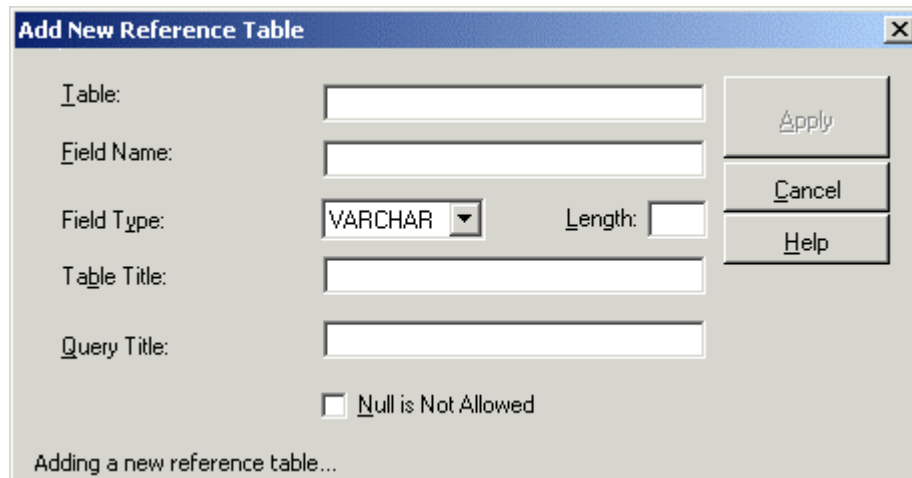
The image shows a Windows-style dialog box titled "Add New Reference Table". It contains several input fields: "Table:" (a text box), "Field Name:" (a text box), "Field Type:" (a dropdown menu currently showing "VARCHAR"), "Length:" (a text box), "Table Title:" (a text box), and "Query Title:" (a text box). To the right of these fields are three buttons: "Apply", "Cancel", and "Help". Below the input fields is a checkbox labeled "Null is Not Allowed". At the bottom of the dialog, there is a status bar that reads "Adding a new reference table...".

Figure 15: Add New Reference Table window

2. In the **Table** field, enter the table name.

Because a table cannot exist without fields, at least one field must be specified for this table.

3. Enter appropriate values in the following fields:

- **Field Name**
- **Field Type**
- **Length**
- **Table Title**
- **Query Title**

By default, the table can include null values.

4. To exclude null values from the table, select **Null is Not Allowed**.
5. To add the table to the list, click **Apply**.

The **List of Reference Tables** window displays the newly created table.

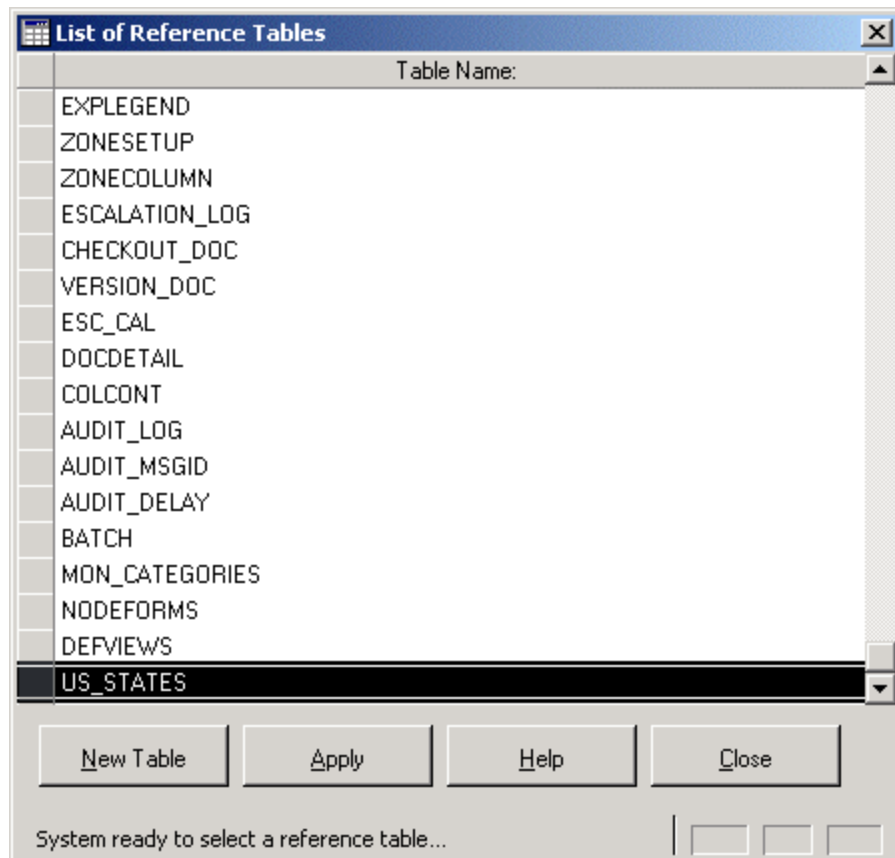


Figure 16: Reference table in List of Reference Tables window

Specifying Table Settings

To specify table settings, proceed as follows:

1. Select the new table in the list.
2. To open the **List of Reference Fields** window, click **Apply**.

The **List of Reference Fields** window appears.

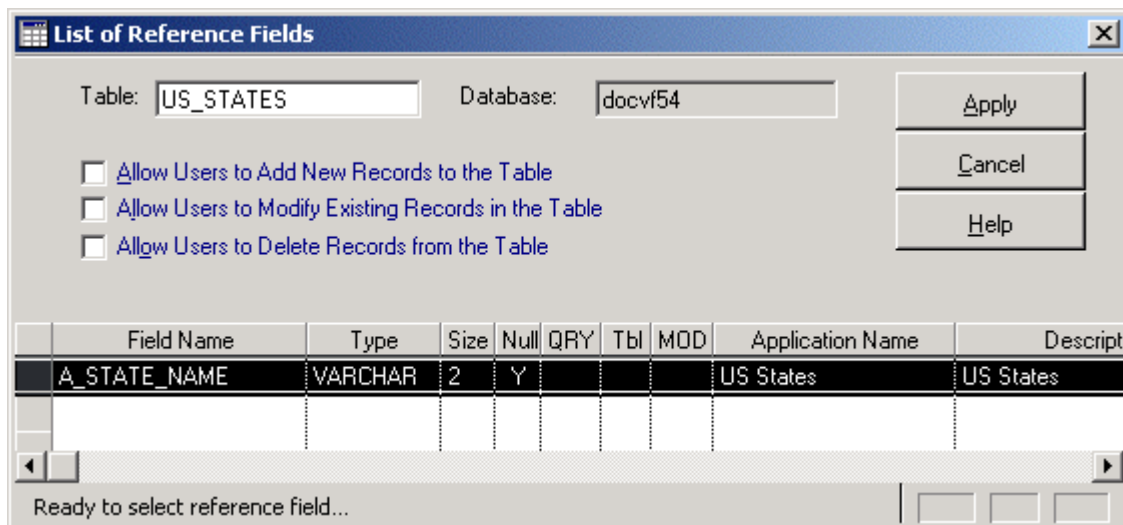


Figure 17: List of Reference Fields window

The **List of Reference Fields** window displays the table name, the database in which it was created, and the field entered. The system automatically defines the field as allowing null values, and this cannot be changed.

3. To specify the permissions of users to work with records in the table, select the appropriate options.

The following options are available:

- **Allow Users to Add Records to the Table**
- **Allow Users to Modify Existing Records in the Table**
- **Allow Users to Delete Records from the Table**

The preceding options allow values to be changed in the reference table only while users are working in workflow objects.

4. To change the settings for the **Qry**, **Tbl**, and **MOD** columns, return to the **Project Table Maintenance** window.
5. If there is more than one field in the table, select the field to use for the reference table and click **Apply**.

If the reference is based on a custom table, the **Values** button appears for the selected field.

Modify Field

Table: FOLDER

Field Name: A_STATE

Field Type: VARCHAR Length: 2

Input Mask:

Table Title: A_STATE

Query Title: A_STATE

Field attributes

- ☐ Null is Not Allowed
- ☒ Part of the Unique Index
- ☒ Appears in the Query Window
- ☒ Appears in the Table Window
- ☒ Appears in the Modify Window
- ☒ Create/Modify by Reference
- ☐ Word In Text Index

Modifying field A_STATE

Figure 18: Modify/Add New Field window, with the Values button

- To add values to the reference table, click **Values**.

The table name appears in the title bar.

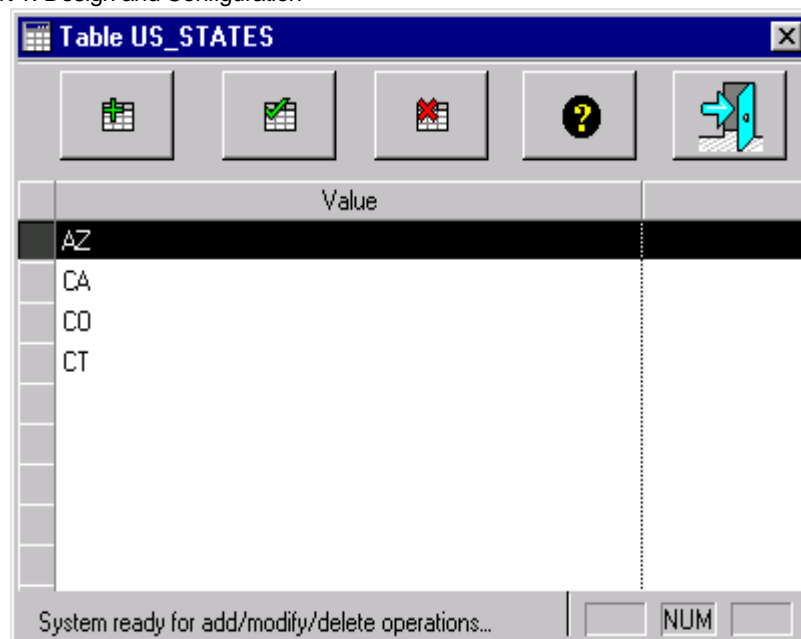


Figure 19: Reference table values

7. To add values, click **New**.



8. In the blank field that appears at the top of the window, enter the value for the table and press **ENTER** or click **Apply**.
9. Repeat the preceding procedure until all required values are entered.
10. To return to the previous toolbar view, click **Close**.

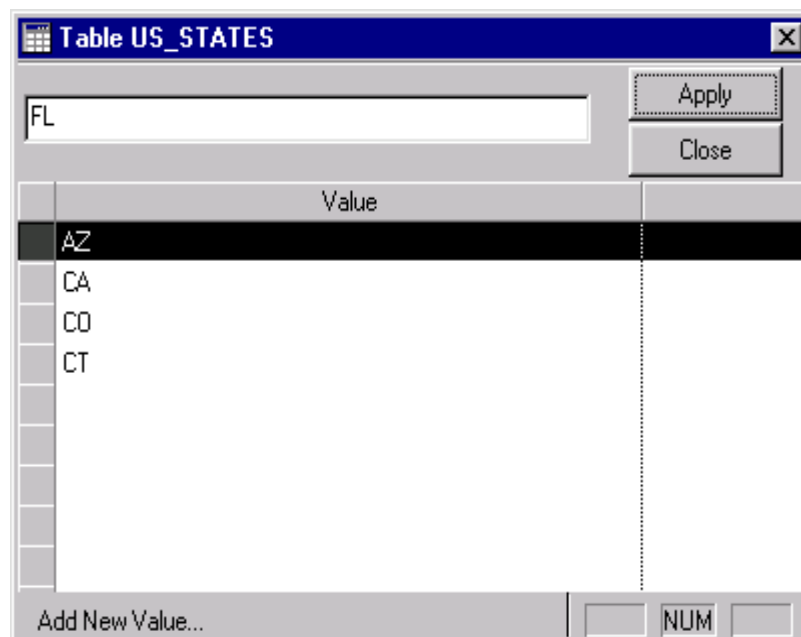


Figure 20: Adding values to the reference table

11. To delete a value, click **Delete**.



12. To modify a value, click **Modify**.



13. To return to the **Modify/Add New Field** window, click **Exit**.

Copying Tables

Tables in the **Project Table Maintenance** window can be copied and exported to external applications, for example, to Excel or Word. This feature is useful for creating reports.

To copy and export a table, proceed as follows:

1. In the **Project Table Maintenance** window, select **Edit > Copy Table** or press **CTRL+C**.

The table contents are copied to the clipboard.

2. To export the copied data, open a document in an external application.
3. Press **CTRL+V**.

The contents of the table appear in the document.

Managing Views

A view is created using a SQL statement. It contains functions, or filtering conditions, that perform a selection in one table or several tables. In Exigen Workflow, a view or several views are assigned to a project table to limit access to data for certain categories of users or workflow nodes.

Views are useful when different users must treat fields in a table differently. For example, users belonging to a certain security group can be restricted to modify a field in a table. Fields can be excluded from certain workflow nodes. Limiting access to data is done by defining rules about how table fields appear in different Exigen Workflow objects windows. For information on rules, see [Setting Conditions](#).

A window type is defined when you add or modify it. For more information on window types, see [Adding and Modifying Fields](#). Views can be used to manage how fields appear to different security groups and workflow nodes and objects. For more information on views, see [Setting Conditions](#).

The following three concepts define a view:

- table name assigned to the view
- window mode related to the view
- view selection statement, defined using SQL

Note: In this Exigen Workflow version, views can be assigned only to the system table SYSCOLUMNS.

The following four window types are defined for Exigen Workflow objects:

Window types	
Type	Description
Modify	Used to enter or update data.
Query	Used to search data.
System	Used within the system.
Table	Used to display data.

The following topics are described in this section:

- [View Management Window](#)
- [Creating and Modifying Views](#)
- [Setting Conditions](#)

View Management Window

To open the **View Management** window, in the **Project Maintenance** window, select **Maintenance > Manage Views**. The **View Management** window appears.

View Management

Table: FOLDER ☒ Is Column View Window Mode: Modify

View List

View Name	Description
FOLDER_M001	

Buttons: New, Modify, Delete, Set Conditions, Show Conditions, Close, Help

Figure 21: View Management window

The following table describes the data fields in the **View Management** window:

View Management window data fields					
Field	Description				
Table	Lists all the Exigen Workflow project tables. If you selected a table in the Project Table Maintenance window, it is also selected in the combo box. For information on the Project Table Maintenance window, see Project Table Maintenance Window .				
Is Column View	<p>Indicates if the view selected in View List is based on SYSCOLUMNS table.</p> <table> <tr> <td>Selected</td><td>Yes</td></tr> <tr> <td>Cleared</td><td>No</td></tr> </table> <p>This check box is disabled and selected because this version of Exigen Workflow supports only column views.</p>	Selected	Yes	Cleared	No
Selected	Yes				
Cleared	No				
Window Mode	<p>Lists all window modes:</p> <p>Modify</p> <p>Query</p> <p>System</p> <p>Table</p>				

The list of views that appears in the **View List** table depends on the values you select in the **Table** and **Window Mode** fields.

The **View List** table consists of the following two columns:

View List table	
Column	Description
View Name	View name. Set automatically when creating the view.
Description	View description. Set when creating or modifying the view.

To perform basic operations with views, proceed as follows:

1. To create, modify, or delete a view, click **New**, **Modify**, or **Delete**.

For more information on views, see [Creating and Modifying Views](#).

2. Select a view and click **Set Conditions**.

The **View Usage Properties** window with all conditions set for the view appears. For more information on conditions, see [Setting Conditions](#).

3. To open the **Views and Conditions** window, select **Show Conditions**.

The **Views and Conditions** window displays a list of all views with their set conditions. It is also possible to add, modify, and delete views in this window.

4. To edit existing conditions for the field, click **Set Conditions**.
5. To close the **Views and Conditions** window and redisplay the **View Management** window, click **Hide Conditions**.

Creating and Modifying Views

To add a new view to the table SYSCOLUMNS, proceed as follows:

1. In the **View Management** window, click **New**.

The **Create View** window appears.

Figure 22: Create View window

Because views are created for the SYSCOLUMNS table, the **Is Column View** check box is set to Y by default.

A view name is automatically set in the **View Name** field. It has the following structure:

View name structure	
View name	Components description
FOLDER	First letters of the table name. Eight characters is the maximum length of this segment.
_	Underscore.
C	Column view. If there is a letter between the underscore and the window mode, it is a column view.

View name structure									
View name	Components description								
T	Window mode: <table border="1"> <tr><td>M</td><td>Modify</td></tr> <tr><td>Q</td><td>Query</td></tr> <tr><td>S</td><td>System</td></tr> <tr><td>T</td><td>Table</td></tr> </table> <p>The letter changes automatically as the window mode is changed in the Window Mode drop-down combo box.</p>	M	Modify	Q	Query	S	System	T	Table
M	Modify								
Q	Query								
S	System								
T	Table								
002	View number.								

If a view is selected in the **View Management** window, the SQL statement for the selected view appears in the **SQL Statement** window. The following table lists the default column view statements for the FOLDER table for each window mode:

View statements	
Window mode	SQL statement
Modify	select * from A01_SYSCOLUMNS where (MDF not in ('N', 'n') or MDF is NULL) and (TBNAME in ('FOLDER'))
Query	select * from A01_SYSCOLUMNS where (QRY not in ('N', 'n') or QRY is NULL) and (TBNAME in ('FOLDER'))
System	select * from A01_SYSCOLUMNS where (TBNAME in ('DOCUMENT'))
Table	select * from A01_SYSCOLUMNS where (TBL not in ('N', 'n') or TBL is NULL) and (TBNAME in ('FOLDER'))

- In the **SQL Statement** window, enter your own statement and a description in the **Description** field, as in the following examples:

SQL statements	
Statement	Description
select * from XXX_SYSCOLUMNS where MDF = 'Y' and TBNAME = 'DOCUMENT' and NAME not in ('A_MYFIELD1', 'A_MYFIELD2')	Selects the SYSCOLUMNS table fields, where TBNAME field value is DOCUMENT and NAME field value is neither A_MYFIELD1 nor A_MYFIELD2, and which are set to appear in the Modify Window as described in Adding and Modifying Fields .
select * from XXX_SYSCOLUMNS where QRY = 'Y' and TBNAME in ('FOLDER') and not (NAME = 'A_F1')	Selects the SYSCOLUMNS table fields, where TBNAME field value is FOLDER and NAME is not A_F1, and which are set to appear in the Query window as described in Adding and Modifying Fields .

Note: Only custom fields can be hidden.

- When the SQL statement is complete, to view the result of the statement, click **Check SQL**.

A table listing all data found based on the statement is displayed. The columns in the **Check SQL** table are the same as the fields in the SYSCOLUMNS table.

Note: It is strongly recommended that you use 'select *' as a column definition for column view. Most Exigen Workflow objects use all columns of the SYSCOLUMNS table internally to find properties of tables' fields. To exclude a field, use a 'where' clause of a SQL statement.

4. To modify an existing view, in the **View Management** window, select a view and click **Modify**.

The **Edit View** window appears. Only the **SQL Statement** and **Description** fields can be edited in the **Edit View** window.

5. To delete a view, in the **View Management** window, select the view and click **Delete**.

The window prompting you to delete the view appears.

Setting Conditions

View conditions are used to determine the following:

- objects and workflows in which the particular view can be used
- users from security levels that can use the view

When a view is defined, a default view usage condition is automatically set. The condition defines that users from all security levels can use the view in all objects and nodes in any workflow. View conditions can be set when creating the view or after the view is created.

1. To set view conditions, in the **View Management** window, select the view and click **Conditions**.

The **View Usage Properties** window appears.

View Usage Properties

Table: FOLDER

Is Column View: Y

View Name: FOLDER_CM001

Window Mode: Modify

Description:

Conditions For This View

	Level	Object Type	Workflow	Node
	All	All	All	All

Add Delete Apply Close Help

Figure 23: View Usage Properties window

View conditions are set for the following:

View conditions	
Parameter	Description
Level	Exigen Workflow security levels.
Object Type	Exigen Workflow object type.
Node	Exigen Workflow project's workflow node.
Workflow	Exigen Workflow project's workflow.

- To create a new condition, click **Add**.

For each condition parameter, a drop-down combo box appears with the default value **All**.

- In the drop-down combo boxes, select the following:
 - user group
 - user type
 - workflow node
 - workflow you want the view to be applied to

It is possible to create several conditions for one view. For example, you can assign one view to several user groups.

Note: If any parameter differs from the required one, this condition is ignored. For example, in workflow Wfl2, all conditions whose workflow parameter is not set to Wfl2 or All are ignored.

4. To apply changes, click **Apply**.

Because several view condition parameters are available, ambiguous situations can occur.

For example, the following two views have the following conditions:

- View 1: Level = All, Object = Retrieve, Node= All, Workflow= All
- View 2: Level= All, Object= All, Node= All, Workflow= Wfl1

It is difficult to decide which view must be used in the Retrieve node, because the condition for View 1 says all Retrieve objects can use it, but View 2 condition says it can be used in all nodes in a particular workflow.

To eliminate confusion, weight coefficients are used. If a parameter value for a condition is specified, for example, object type is set to **Retrieve**, not **all**, a hard-coded weight coefficient is set for the parameter. If the value is **All**, the coefficient is 0. All the parameter values are summed defining a weight of the condition. A condition with the largest weight is selected. A view with the selected condition is used. Coefficients for each parameter are set as follows:

Coefficients	
Parameter	Coefficient
Level	3.0
Workflow	1.2
Node	1.1
Object Type	1.0

In our example the following applies:

- View 1: Level = All, Object= Retrieve, Node= All, Workflow= Current
- View 2: Level= All, Object= All, Node= Current, Workflow= Current

Coefficient sum:

- For View 1: $1.0 + 1.2 = 2.2$
- For View 2: $1.1 + 1.2 = 2.3$

Because the sum is greater for View 2, it is used in the current node of the current workflow.

Note: It is not possible to assign two identical conditions to one view. An error message is displayed if you try to apply two identical conditions to one view.

Defining Batch Status Option

The batch status can be assigned to a batch after it is scanned into the system. The batch status value can be used for defining routing rules. For information on routing rules, see [Setting Up Workflow Routing Rules](#).

If the batch status concept is assigned for a project, the **Routing Info** drop-down list box appears in the **Scan Dialog**, as described in the *Exigen Workflow User's Guide*, Chapter 3: High Volume Scanning, Scan Dialog Window.

Note: This functionality can be set only to the Exigen Workflow Client/Server version.

To define the batch status option for a project, proceed as follows:

5. In the **Project Builder** window, select a project and click **Project Maintenance**.
6. Select **Maintenance > New Table**.
7. In the **Add New Project** table, enter the following values:

Add New Project table values	
Field	Value
Table	BATCH_STATUS.
Field Name	A_STATUS.
Field Type	VARCHAR.
Length	Maximum number of symbols a value of the status can have.

By default, the table can include null values.

8. To exclude null values from the table, select **Null is Not Allowed**.
9. Click **Apply**.
10. In the **Project Table Maintenance** window, in the table list, select the BATCHPARCEL table.
11. Add a new field to the BATCHPARCEL table named A_BATCH_STATUS of the VARCHAR type and the same length as the A_STATUS field.

All other options depend on your particular needs.

To add batch status values to the project, proceed as follows:

1. In Exigen Workflow Explorer, select **Administration Tools > Workflow Tools > Administrator**.

The **Administrator Utilities** window appears.

2. In the **Administrator Utilities** window, select the project and click **Table Maintenance**.
3. In the **Table Maintenance** window, select the BATCH_STATUS table and click **Run**.
4. To add a batch status value, in the **BATCH_STATUS** window, click **New Record**.
5. In the **New Record** window, enter a batch status value and click **OK**.
6. To add as many batch status values as needed, repeat steps 4 and 5.

You can now assign the added batch status values to a batch when scanning. The batch status values can be used for defining routing rules. For information on routing rules, see [Setting Up Workflow Routing Rules](#).

Setting Internal Counters

Internal counters generate record sequential numbers (RSNs) for new records in database tables. For example, when a new document is scanned into the system, it is assigned an RSN according to the current internal counter value. Administrators can adjust internal counters if the default generated RSNs are not appropriate.

To set counters for project tables, proceed as follows:

1. In the **Project Table Maintenance** window, select **Maintenance > Check Internal Counters**.

The **Set Internal Counters** window appears.

Field	Value	MAX(RSN)
Folder:	1	1
Subfolder:	2	2
Document:	100	4
Archive:	0	
Batch/Parcel:	3	3
Batch:	1	
Retention:	0	
Event:	0	
Docdetail:	0	
Task Instance:	0	
ACL Entitlement:	0	
ACL Permission:	0	
ACL Privilege:	0	
Task Status:	0	
Task History:	0	
Taskflow Inst.:	0	

Figure 24: Viewing internal counters

The **Project** field displays the project ID and name. The **Counters** section lists all project tables for which internal counters can be configured.

For Oracle databases, the left column displays the internal counter value and the right column displays the last assigned RSN value in the project table.

For non-Oracle databases, the left column displays the internal counter value plus one and the right column displays the next RSN value to be assigned for a new record in the project table.

If there is no value displayed in the right column, there are no records in the table.

Sequences are used to implement counters in Oracle databases. The database server allocates 20 sequence numbers by default. As a result, the left column in the **Counters** section can display slightly larger numbers than are actually used.

2. If an Oracle database is used, in the **Counters** section, set the values in the left column so that they exceed those in the right column by at least one.

For example, if the **MAX(RSN)** value for documents is 14, the **Document** value must be at least 15.

3. If a non-Oracle database is used, in the **Counters** section, set the values in the left column so that they are greater than or equal to the values on the right.
4. To apply changes and close the window, click **Apply**.

Recreating Project Indexes

To recreate all project indexes that are registered in the SYSINDEXES or SYSKEYS tables, proceed as follows:

1. In the **Project Table Maintenance** window, select a project.
2. Select **Maintenance > Recreate Project Indexes**.

This option recreates all project indexes for all project tables. If an index already exists in the database, it is deleted and recreated. If an index does not exist but is registered in the SYSINDEXES or SYSKEYS tables, it is created in the database.

Exigen Workflow Security

Exigen Workflow security controls user access to Exigen Workflow applications, operations within each application, documents, folders, and subfolders.

User IDs and passwords control access to Exigen Workflow.

Security schemes ensure that documents, folders, and subfolders are retrieved, viewed, and modified only by authorized users and user groups. It is possible to apply security to a document, folder, or subfolder from the moment it enters the Exigen Workflow system.

The following security schemes are available:

- role based security

- access control list (ACL) based security

The two security schemes are mutually exclusive and cannot be used simultaneously.

The following topics are included in this section:

- [Role Based Security](#)
- [ACL Based Security](#)

Role Based Security

The following topics are described in this section:

- [Role Based Security Concepts](#)
- [Implementing Role Based Security](#)

Role Based Security Concepts

Role based security involves setting up and assigning security levels and access levels:

- A **security level** specifies the rights to set up and monitor the Exigen Workflow system and to work with document annotations and document versions. A security level also defines access rights for workflow objects and defines the tasks that can be performed in workflow objects. Security levels are assigned to users and global user groups.
- An **access level** restricts access to specific folders and subfolders. Access levels are assigned to security groups.

The following table summarizes the role based security control mechanism:

Role based security control mechanism	
Object	Control mechanism
Workflow groups	Control access to workflow objects within Exigen Workflow.
Security levels	Control the ability to perform specific operations in an application, for example, add, modify, delete, retrieve, edit, and hide.
User setup	Controls access to document types, tasks, and jobs.

Implementing Role Based Security

To implement role based security, proceed as follows:

1. Ensure that role based security is activated as described in [Security Tab](#).

Note: Role based security is activated by default.

2. Set up global user groups as described in [Setting Up Global User Groups](#).
3. Set up workflow groups as described in [Setting Up Workflow Groups](#).
4. Specify security levels as described in [Specifying Security Levels](#).

5. Specify access levels as described in [Specifying Access Levels](#).

ACL Based Security

ACL based security defines the rights of users and global user groups to work with particular documents, folders, and subfolders.

The following topics are included in this section:

- [ACL Based Security Concepts](#)
- [Implementing ACL Based Security](#)

ACL Based Security Concepts

In the ACL based security scheme, an **access control list** defines the rights of users and user groups to retrieve and work with documents, folders, and subfolders.

The following general procedure is used to implement ACL based security:

1. Users and global user groups are set up.
2. ACL based security is activated.
3. ACL based security objects are set up. This sets up document access control by defining rules for accessing documents, folders, and subfolders.
4. A set of allowable tasks is defined for workflow nodes.
5. Security is defined for individual documents, folders and subfolders in nodes. The ACL list becomes visible to the user.

Exigen Workflow offers the possibility of automatically assigning security to newly created documents, or applying security to documents when they arrive in a designated workflow node. For example, a company with many branch offices sends documents to a central Exigen Workflow system. These documents are routed to Automatic Queue Server, which assigns security to each document and routes the document to the next workflow node.

For more information on using Automatic Queue Server to assign security, see the *Exigen Workflow Administrator's Guide, Part 2: Business Component Reference*, Chapter 19: Automatic Queue Server, Using Automatic Queue Server to Apply Security.

The following table describes ACL based security concepts:

ACL based security concepts	
Concept	Definition
resource	Entity, such as a document, folder, or subfolder, to which access control is applied.
security subject	User or global user group.

ACL based security concepts																			
Concept	Definition																		
privilege	<p>Subset of system resources combined with a subset of functions that can be performed on them.</p> <p>For example, a privilege can be the right to read and modify documents having the document type Medical Bill.</p>																		
entitlement	<p>Mechanism for defining a subset of resources associated with a privilege. An entitlement defines the resource subset based on resource attributes.</p> <p>For example, an entitlement defines a subset of documents of type Medical Bill.</p>																		
filter	Entitlement.																		
permission	<p>Authorization to perform a particular operation on a resource. A permission can include one or more operations. The operations can be standard or customized.</p> <p>The following standard operations are available:</p> <table> <tr> <th>Operation</th><th>Description</th></tr> <tr> <td>read</td><td>Read resource properties in the Exigen Workflow database.</td></tr> <tr> <td>modify</td><td>Modify the resource in the Exigen Workflow database.</td></tr> <tr> <td>delete</td><td>Delete the resource from the Exigen Workflow database.</td></tr> <tr> <td>view</td><td>View document contents.</td></tr> <tr> <td>edit</td><td>Modify document contents.</td></tr> <tr> <td>hide</td><td>Create and maintain hidden areas in the document.</td></tr> <tr> <td>grant</td><td>Grant security rights.</td></tr> <tr> <td>create children</td><td>Create a child object. For example, in a folder, a document can be created.</td></tr> </table>	Operation	Description	read	Read resource properties in the Exigen Workflow database.	modify	Modify the resource in the Exigen Workflow database.	delete	Delete the resource from the Exigen Workflow database.	view	View document contents.	edit	Modify document contents.	hide	Create and maintain hidden areas in the document.	grant	Grant security rights.	create children	Create a child object. For example, in a folder, a document can be created.
Operation	Description																		
read	Read resource properties in the Exigen Workflow database.																		
modify	Modify the resource in the Exigen Workflow database.																		
delete	Delete the resource from the Exigen Workflow database.																		
view	View document contents.																		
edit	Modify document contents.																		
hide	Create and maintain hidden areas in the document.																		
grant	Grant security rights.																		
create children	Create a child object. For example, in a folder, a document can be created.																		
security entry	<p>Combination of a privilege, a permission, and a user or global user group.</p> <p>For example, User Group 1 has read-only permission for medical reports.</p>																		
access control list	<p>List containing a set of access control entries that define the security policy associated with a resource.</p> <p>For example, an access control list can include all of the users and global user groups having access to a particular folder. Administrators are assigned the right to view and edit documents. Reviewers are assigned the right to view documents.</p>																		
ACL	Access control list.																		
access control entry	<p>Combination of a resource ID and a privilege.</p> <p>For example, the resource is a folder containing recently prepared medical bills. The privilege is to verify the bills and send them.</p> <p>Access control lists are composed of access control entries.</p>																		
ACE	Access control entry.																		

Implementing ACL Based Security

To implement ACL based security, proceed as follows:

1. Set up users and global user groups.

For information on setting up users, see [Setting Up Users](#).

For information on setting up global user groups, see [Setting Up Global User Groups](#).

2. Activate ACL based security.

For information on activating ACL based security, see [Security Tab](#).

3. Set up document access control by specifying security objects.

For information on setting up document access control, see [Setting Up Document Access Control](#).

4. Assign tasks to workflow nodes.

For example, the administrator can specify whether documents can be added, modified, deleted, or retrieved in the given node.

For information on setting up tasks for workflow nodes, see [Additional Settings Tab](#).

5. Define security for individual documents, folders, and subfolders in nodes.

In all workflow nodes except High Volume Scan, security can be assigned to individual resources.

For more information on defining security settings for resources in a node, see the *Exigen Workflow User's Guide*, Chapter 4: High Volume Indexing, Specifying Document, Folder, and Subfolder Security Settings.

6. If there is a requirement to automatically assign security to all documents arriving in a node, set up automatic security assignment as described in the *Exigen Workflow Administrator's Guide, Part 2: Business Component Reference*, Chapter 19: Automatic Queue Server, Using Automatic Queue Server to Apply Security.

Implementing ACL based security affects the operations that users and user groups can perform on documents, folders, subfolders, and parcels. For a list of restrictions, see [Appendix H: How ACL Based Security Affects Documents, Folders, and Subfolders](#).

Setting Up Document Versioning

When setting up a project, document versioning can be enabled. Document versioning is a feature that allows Exigen Workflow to maintain various versions of the following types of documents:

- document images created in Exigen Workflow
- task documents created by external applications such as Word

Document versioning is not supported for ERM documents.

If document versions are available, users with appropriate document versioning access rights can perform the following tasks:

- view a document version

- delete a document version
- designate a document version as current

The current document version is opened by default and processed in Exigen Workflow.

To set up document versioning, proceed as follows:

1. In the **Project Configuration** tool, in the **Document Management** tab, enable the checkin/checkout feature as described in [Document Management Tab](#) in [Configuring the Project](#).
2. Enable document versioning as described in [Document Management Tab](#) in [Configuring the Project](#).
3. To grant document versioning access rights to the user, using the Administrator tool, select **Administrator > System Setup > Setup > Security Levels > Add or Modify**.
4. To set access rights for the user, in the **Document version control** area, select one or more of the following options:
 - **View versions**
 - **Activate versions**
 - **Delete versions**

For more information on setting user access rights, see [Specifying Security Levels](#).

For information on working with document versions, see the *Exigen Workflow User's Guide*, Appendix B: Document Versioning.

Configuring the Project

After creating a project and defining project tables and fields, you must configure the project. Remember that you can always add new tables and table fields to your project.

To configure the project, click **Project Configuration**.



The **Project Configuration** window displays the project name in the title. The following tabs are available:

- [Location Tab](#)
- [Indexing Tab](#)
- [QA Tab](#)
- [Optical Tab](#)
- [Document Management Tab](#)
- [Email Tab](#)
- [E-Forms Tab](#)

- [Security Tab](#)

Location Tab

To set the default document location, select the **Location** tab.

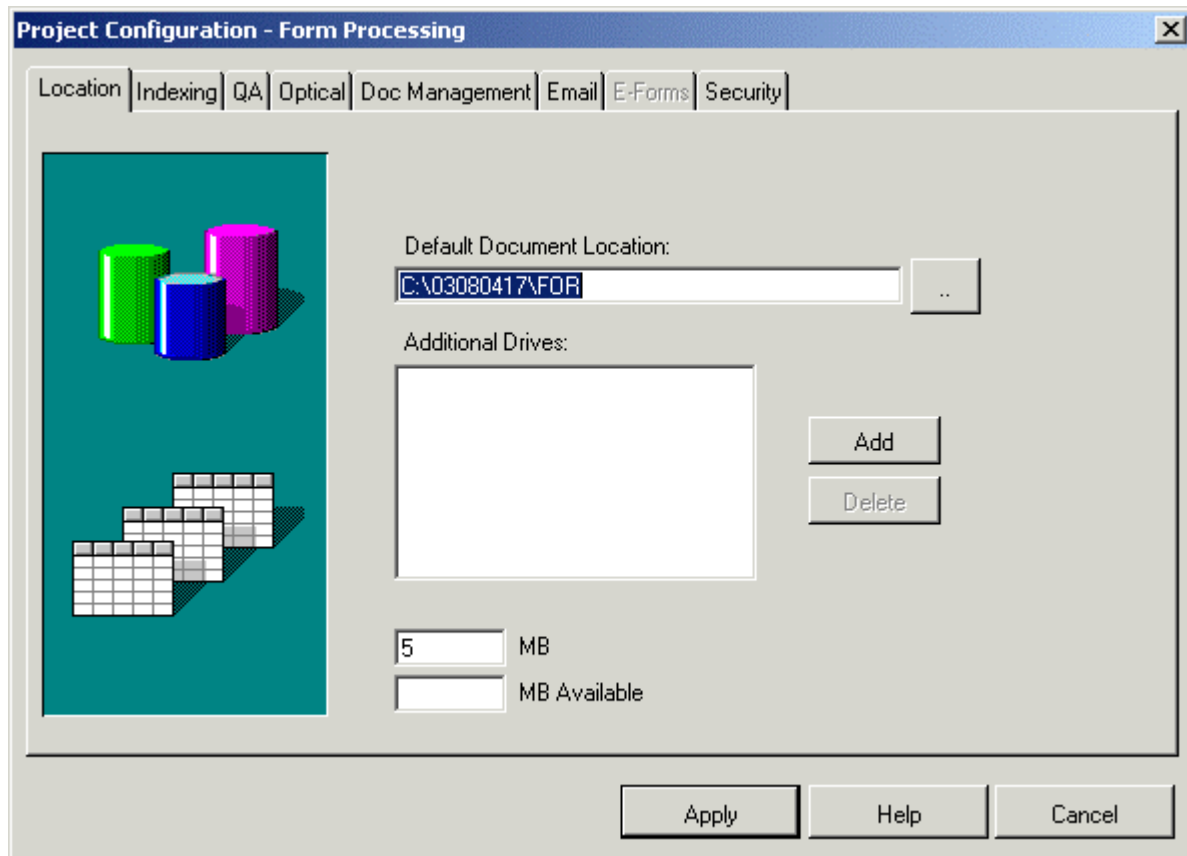


Figure 25: Project Configuration window, Location tab

To specify location settings, proceed as follows:

1. To assign the default scan location, click the browse button next to the **Default Document Location** field.



Note that the three-character project ID appears at the end of the path.

Note: The path to the default document location cannot exceed 60 characters.

2. Click **Apply**.

The system prompt asks if you want to add the directory.

3. Click **Yes**.

Mapping scanned images to a directory identified by its project ID makes searching for them easier if you are scanning documents into more than one project.

Additional Drives are used when a user has different drives for storing documents. The system can automatically switch storing documents to the next available drive when the previous drive is full. Additional drives information is not linked to any particular project because storage space is common for all projects. This information appears for every project.

4. To list, assign, or remove additional drives for the scanned images, click **Add** or **Delete** to the right of the **Additional Drives**.

Only drive letters can be selected.

5. In the **MB** field, enter the minimum amount of space needed in the selected drive and on the local drive.

The default value is 5 MB.

6. In the **MB Available** field, enter the total amount of space available.

The space on the local drive must also be taken into account because images are stored locally during the scanning process until they are saved and sent to the next queue. The system checks available space on the selected scan drive before starting the actual scanning. There must be enough space for at least one scanned document to be saved as a file.

7. Click **Apply**.

Indexing Tab

The **Indexing** tab determines the levels at which indexing occurs.

By setting indexing levels, you ensure that documents are not routed through the system without the required values being entered.

To set indexing levels, proceed as follows:

1. Select one of the following options:

Indexing tab options	
Option	Description
Assign Document to Folder, Subfolder and Document Type	Ensures that all documents are assigned values in all three table levels. The Indexing queues have specific windows designed to ensure that all required fields are entered and that the user cannot send the documents to the next queue until they are complete.
Assign Document to Folder and Document Type	Forces indexing at the folder and document level only. This scenario is recommended if you are not using subfolders but want to easily identify different types of documents. This is a default option.
Assign Document to Folder	Indexes only at the folder level.

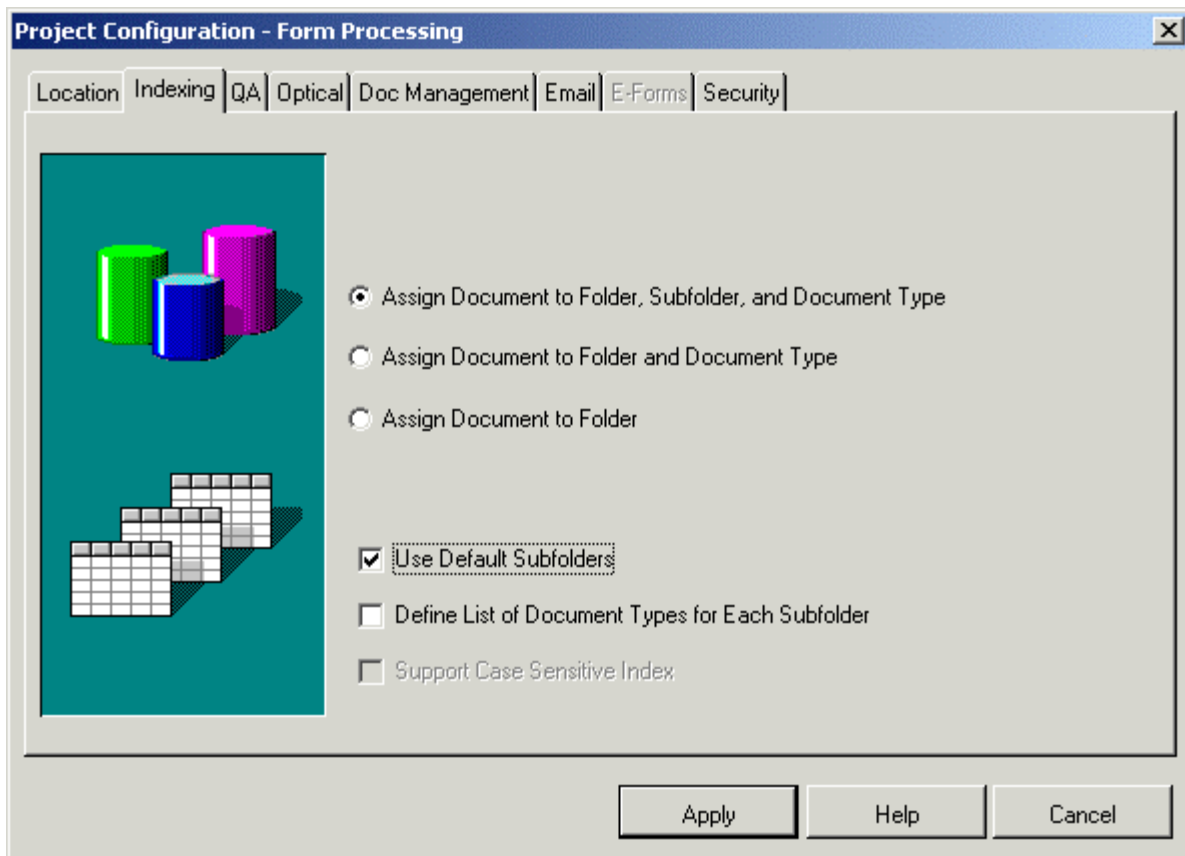


Figure 26: Project Configuration window, Indexing tab

2. Select the appropriate options:

- **Use Default Subfolders**
- **Define List of Document Types for Each Subfolder**
- **Support Case Sensitive Index**

If users must use the default values assigned by the system administrator, select **Use Default Subfolders**. If users can create their own subfolders, do not select this option.

Note: The **Use Default Subfolders** check box appears only when the **Assign Document to Folder, Subfolder, and Document Type** option is selected.

3. To define a list of document types for each subfolder, proceed as follows:

1. To ensure that the SUBFOLDER table contains at least one indexing field, in **Project Builder**, select **Project Table Maintenance**, and open the SUBFOLDER table. If it does not contain at least one indexing field, specify this field.
2. Select **Assign Document to Folder, Subfolder and Document Type**, **Use Default Subfolders**, and **Define List of Document Types for Each Subfolder**.

Note: The **Document Types for Each Subfolder** check box appears only when the **Use Default Subfolders** check box is selected.

3. Click **Apply**.

The system automatically adds a new field named DOC_TYPES to the SUBFOLDER table.

The screenshot shows the 'Project Table Maintenance' window. The 'Project' field is 'INV_Invoice Processing', 'Database' is 'VISIDB', and 'DBS Type' is 'SYBASE'. A dropdown menu is open, showing 'SUBFOLDER' selected. Below the dropdown is a table with the following data:

Field Name	Type	Size	Null	Ind	Qry	Tbl	WIT	Table Title	Query Title
FLD_RSN	INTEGER	4	N					FLD_RSN	Folder #
SUB_FLD_RSN	INTEGER	4	N					SUB_FLD_RS	Subfolder #
SFLD_SEC_RSN	INTEGER	4	Y		N	N		SUB_SEC	SubFld Security
A_NUM	VARCHAR	10	Y	Y	Y	Y	N	A_NUM	A_NUM
DOC_TYPES	VARCHAR	250	Y					DOC_TYPES	Document types

At the bottom of the window is an 'Exit' button.

Figure 27: Subfolder table with DOC_TYPES field

4. To populate the SUBFOLDER table, select **Administration Tools > Workflow Tools > Administrator**, and select the project.
5. Click **Table Maintenance**.
6. Open the SUBFOLDER table that already contains the DOC_TYPES field and add new subfolder records by specifying the field values for each subfolder as follows:
 - Assign FLD_RSN as 999999999.
 - To set the option that defines the list of document types for each subfolder, assign SFLD_SEC_RSN as 0.
 - In the DOC_TYPES field, specify the document types available for this subfolder separated by commas, for example, *Note,Report,Fax,Miscellaneous*. These document types must be defined in the DOCTYPE table.

Support Case Sensitive Index instructs the system to create case sensitive indexes that are used in the Retrieve object for performing case sensitive searches.

Note: Whether this check box is enabled or disabled depends on database case sensitivity.

QA Tab

The **QA** tab is used to configure settings to send random documents to be inspected for quality assurance purposes.

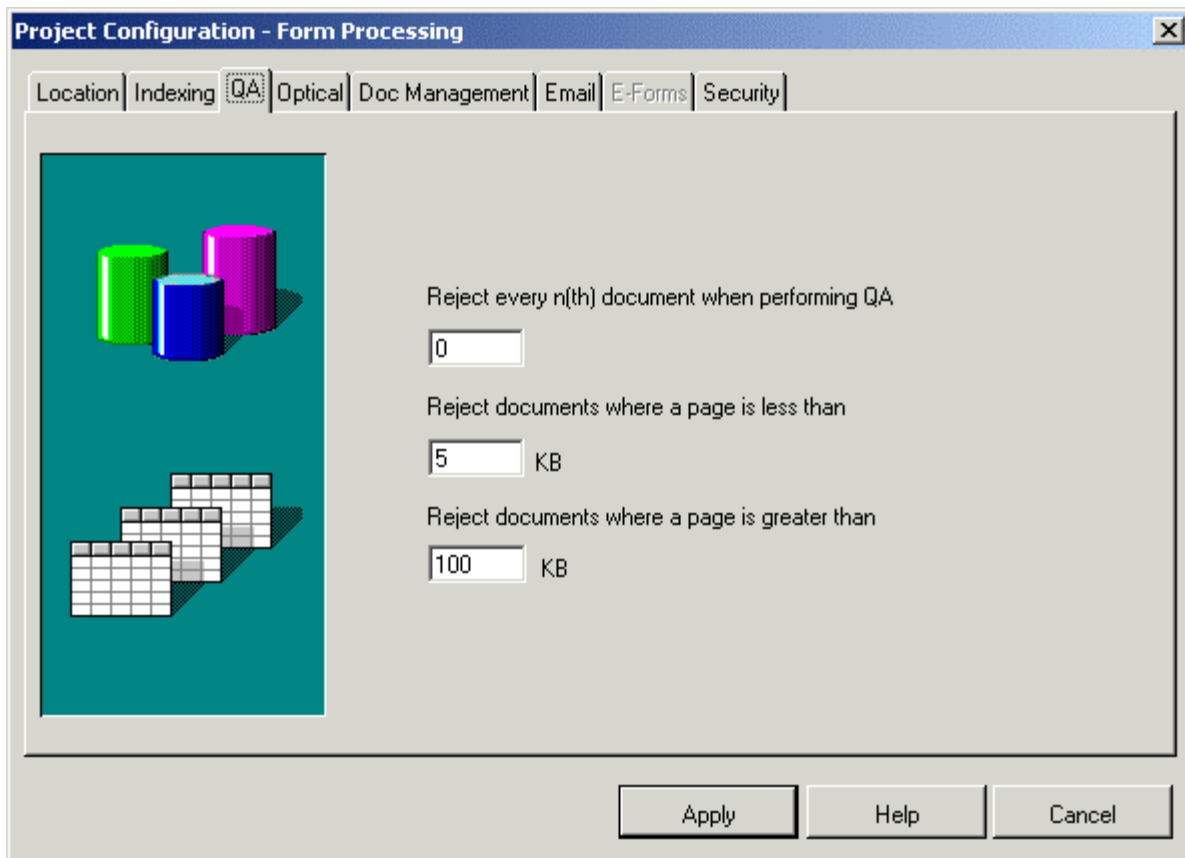


Figure 28: Project Configuration window, QA tab

To identify documents to be sent to the Inspect queue, specify the following **QA** tab settings:

QA tab settings	
Setting	Description
Reject every nth document when performing QA	Integer indicating that each time a multiple of that number is reached, the corresponding document is sent to the Inspect queue.
Reject documents where page is less than 'X' KB	Number of kilobytes indicating that each document in which the size of any page falls below this benchmark is routed to the Inspect queue.
Reject documents where page is greater than 'X' KB	Number of kilobytes indicating that each document in which the size of any page exceeds this benchmark is routed to the Inspect queue.

If you do not want to route documents to the Inspect queue, set the values so that no documents meet the criteria.

You can adjust the settings to include any number of documents.

Optical Tab

In the **Optical** tab, the type of medium where committed documents are sent and record attributes are defined.

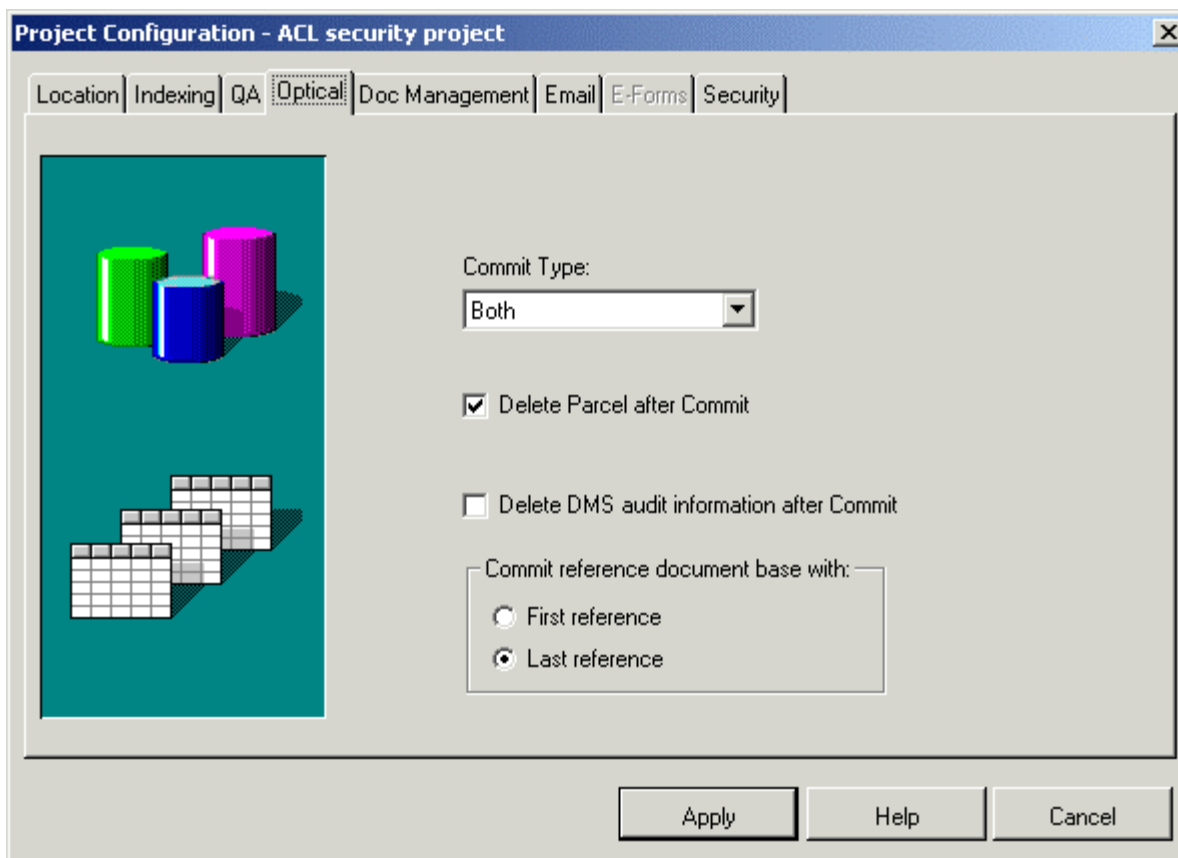


Figure 29: Project Configuration window, Optical tab

To specify settings for committing documents, proceed as follows:

1. In the **Commit Type** list box, select one of the following options:

Commit Type options	
Name	Description
Optical	Defines an optical device as the storage medium.
Server	Selects a server.
Both	Allows both devices to be used for storage.

2. To delete a parcel after commit, select **Delete Parcel after Commit**.

Since parcels are only needed to route documents through the workflow, they must be deleted once the documents are committed to free up space in the database. If documents are pulled from storage back into the workflow, a new parcel is created for them.

3. To clear document audit data after the document is committed, select the **Delete DMS audit information after Commit** box.

All audit information is removed from DMS files.

4. Predefine a system-wide value for this option in the [AUDIT_LOG] section of the visi.ini file. For example, to delete DMS audit information, specify the following setting:

```
[AUDIT_LOG]
DMS_AUD_DEL=YES /* audit data are removed from DMS files */
```

This ensures that the **Optical** tab of the **Project Configuration** window has the **Delete DMS audit information after Commit** box selected for all projects in the system.

If this section is not found, that is, `DMS_AUD_DEL=NO` or the `visi.ini` file contains `DMS_AUD_DEL=NO`, the system uses the specified settings in the **Project Configuration** window.

5. To specify the conditions for committing a document that has reference documents, in the **Commit reference document base with** section, select one of the following options:

Commit reference document base options	
Name	Description
First reference	Original document is committed to storage when the first reference document is committed.
Last reference	Original document is committed to storage when the last reference document is committed.

The **Last reference** option is recommended to ensure that the document remains in the workflow as long as it is being processed. When a document is committed, it is removed from the workflow.

Document Management Tab

The **Doc Management** tab specifies whether the version mechanism is used in the project.

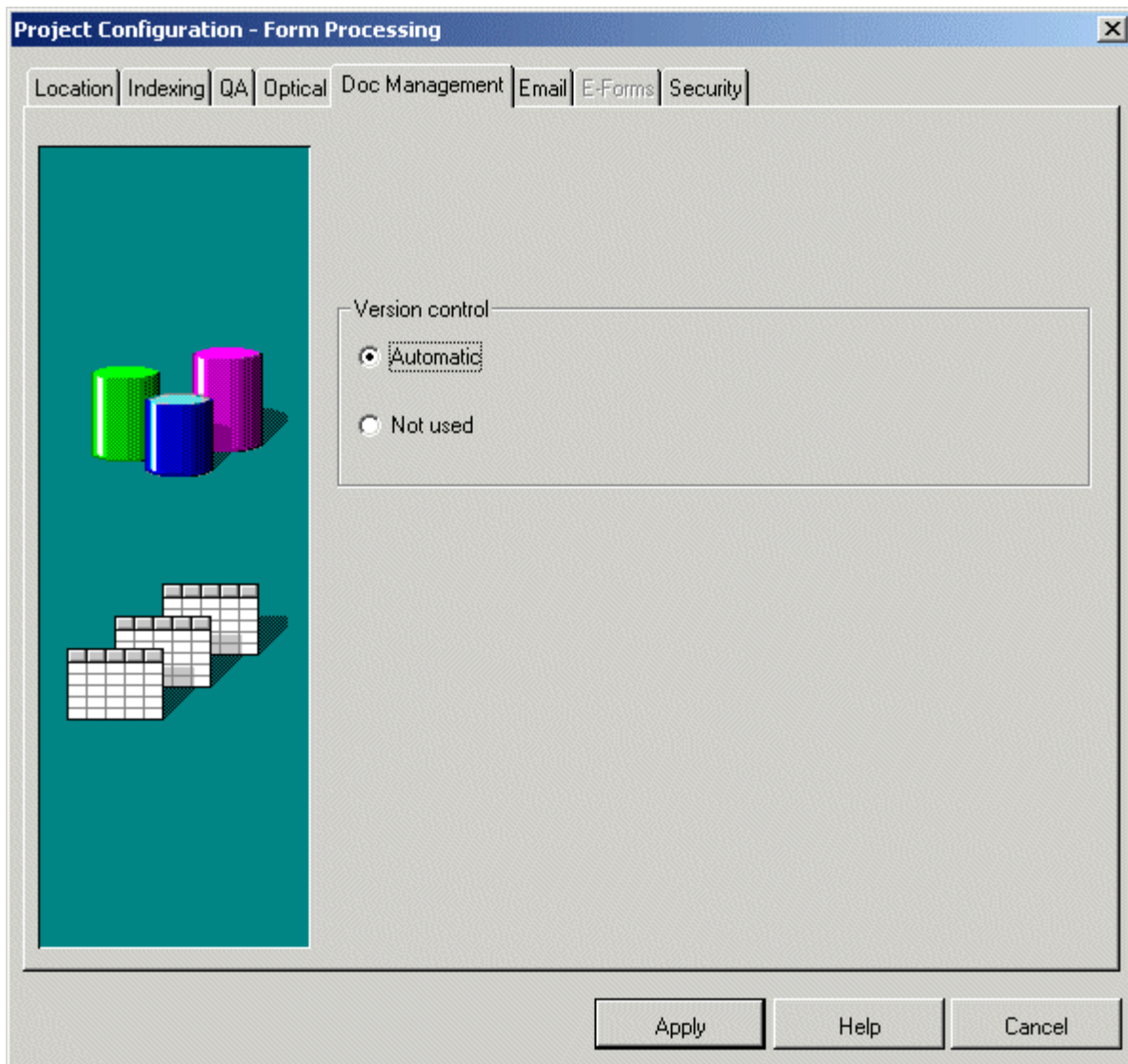


Figure 30: Project Configuration window, Doc Management tab

To use the versioning mechanism in the project, select the **Automatic** option. Otherwise, select the **Not used** option.

If the versioning mechanism is used, Exigen Workflow creates a new document version each time a document is modified. All previous document versions are stored and can be viewed or restored as the current version.

The current document version is opened by default and processed in Exigen Workflow.

Document versioning is not supported for ERM documents.

Email Tab

In the **Email** tab, specify the format in which email is sent.

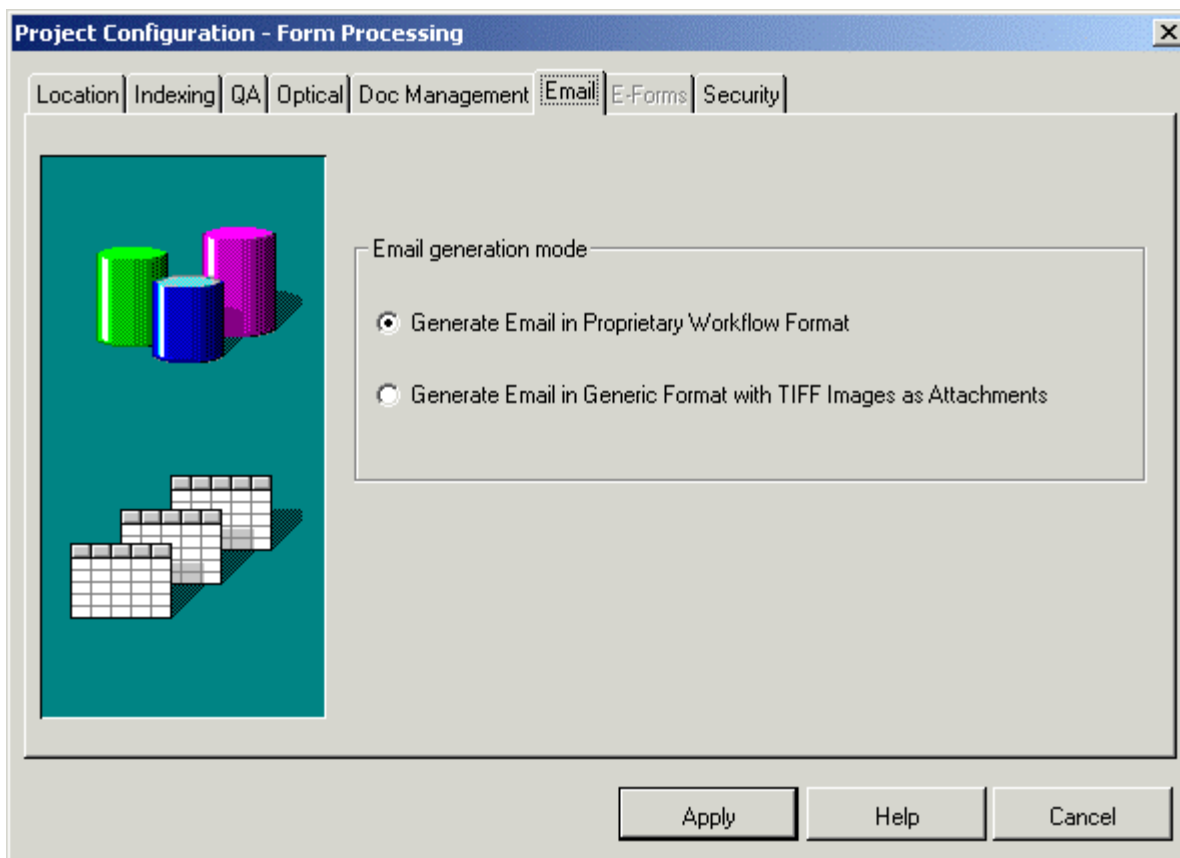


Figure 31: Project Configuration window, Email tab

To set an Exigen Workflow email to be generated in .vis format, **Generate Email in Proprietary Exigen Workflow Format** is selected. This includes both imaged documents and Exigen Workflow database information. For this type of mail, the receiver must have the Exigen Workflow system.

To set an Exigen Workflow email to be generated in a standard email format, with text information and TIFF images as attachments, **Generate Email in Generic Format with TIFF Images as Attachments** is selected. In this case, the recipient does not need the Exigen Workflow system.

Sending emails from Image Viewer can be enabled or disabled by configuring the `visi.ini` file.

To configure the send email functionality in Image Viewer, proceed as follows:

1. Open the `visi.ini` file.
2. If the `[email]` section is not present in the file, add the section.
3. Add or configure the `EnableSendEmail` parameter as follows:
 - To enable the send email functionality in Image Viewer, set the parameter as follows:
`EnableSendEmail=ON`
 - To disable the send email functionality in Image Viewer, set the parameter as follows:
`EnableSendEmail=OFF`

4. Save and close the `visi.ini` file.

E-Forms Tab

In the **E-Forms** tab, to configure how electronic forms are used, proceed as follows:

1. To specify the path to the application server where electronic forms are stored, in the **E-Forms target** field, enter the path in the following form:

```
http://<server>:8080/<application name>/servlet
```

where <server> is the name of the computer on which the application server is installed and <application name> is the application name deployed.

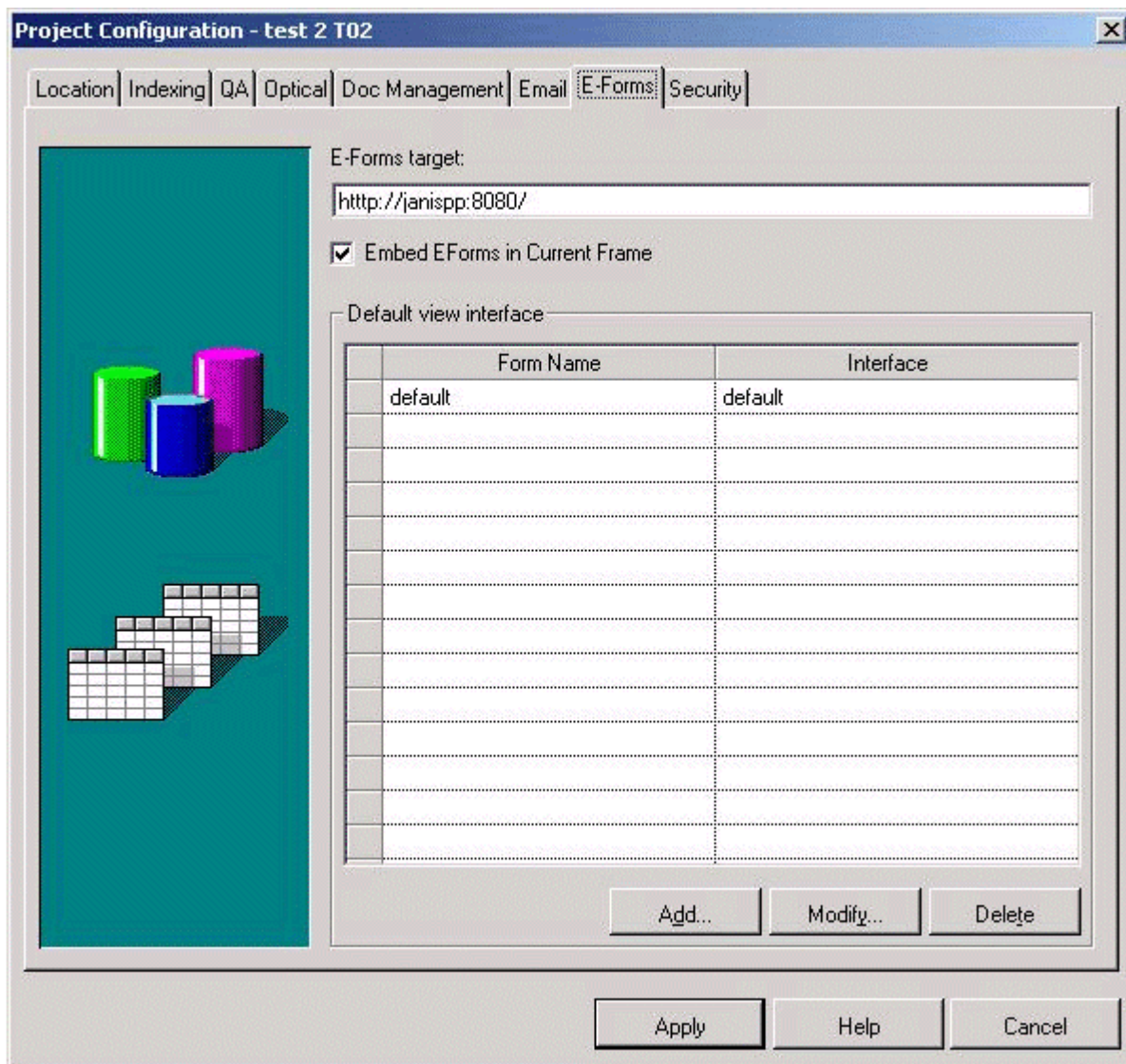


Figure 32: Project Configuration window, E-Forms tab

2. To open forms in the main window, select the **Embed EForms in Current Frame** check box.

If this check box is not selected, the forms are opened in a separate window.

3. To make a new form available to the project, click **Add**.

The **Interface** window appears.

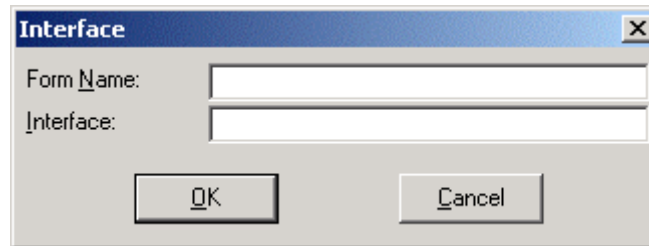


Figure 33: Interface window

4. In the **Form Name** field, enter the form name.

The form name is the name of the form definition of the existing E-Forms document.

5. In the **Interface** field, enter the default interface.

The interface is the interface name to be used with the form definition to launch the form.

6. To add the form, click **OK**.

A new form is added.

7. To modify an existing form, click **Modify**.

The **Interface** window appears.

8. Modify the information in the fields and click **OK**.

9. To delete a form from the project, select the form and click **Delete**.

For more information on Exigen Workflow integration with E-Forms, see [Integrating with Exigen E-Forms](#).

Security Tab

The **Security** tab is used to specify the security scheme for a project and to define permissions for security levels associated with users.

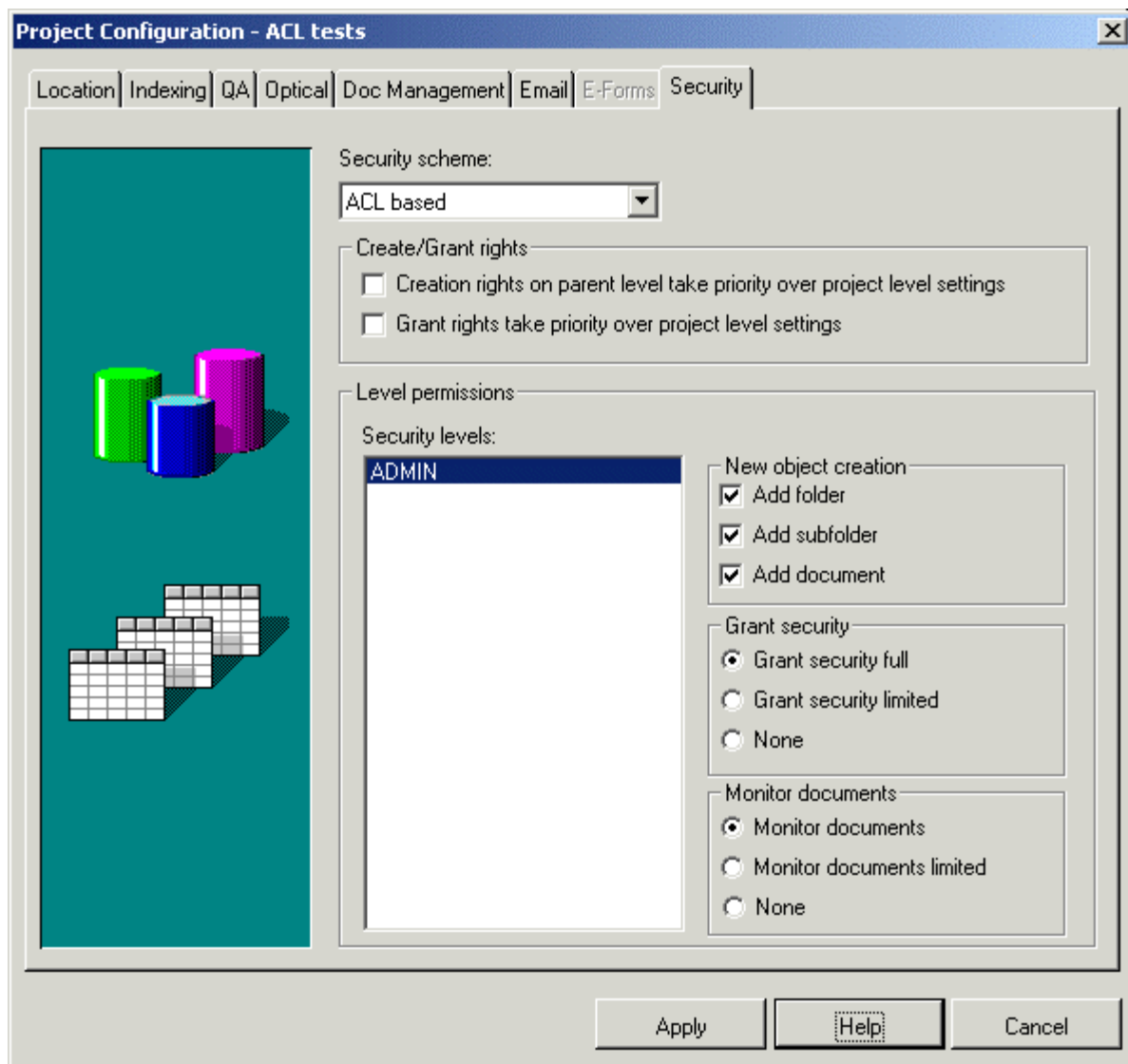


Figure 34: Specifying the security scheme

To specify the security scheme, proceed as follows:

1. In the **Security** tab, in the **Security scheme** field, select one of the following options:

Security scheme options	
Option	Description
ACL based	Uses access control lists to define security.
Role based	Uses security levels and access levels to define security.

For more information on security schemes, see [Exigen Workflow Security](#).

2. If role-based security is selected, to apply the settings and close the window, click **Apply**.
3. If ACL based security is selected, to specify that ACL based security settings determine the rights of users to create subfolders and documents, select **Creation rights on parent level take priority over project level settings**.

If this option is selected, users can create a subfolder only if the appropriate rights are assigned to that user or group for the parent folder. Users can create a document only if the appropriate rights are assigned to that user or group for the appropriate subfolder or folder.

4. To specify that the right to grant ACL based security to a document, folder, or subfolder is determined by ACL based security settings defined for that document, folder, or subfolder, select **Grant rights take priority over project level settings**.

If this option is selected, ACL based security settings for grant rights take priority over project level settings.

5. To set level permissions for a user or global user group, in the **Security levels** field, select a user or global user group.
6. To set level permissions for the selected user or global user group, in the **Level permissions** section, select the required options.

The following options are available:

Level permissions options	
Option	Description
Add folder	Users assigned to the selected security level can add a folder.
Add subfolder	Users assigned to the selected security level can add a subfolder.
Add document	Users assigned to the selected security level can add a document.
Grant security full	Users assigned to the selected security level can grant ACL based security rights for all documents, folders, and subfolders in the project.
Grant security limited	Users assigned to the selected security level can grant ACL based security rights only for those documents, folders, and subfolders to which the user has access. Only privileges possessed by the user can be assigned to documents.
None	Users assigned to the selected security level have no rights to grant ACL based security rights.
Monitor documents	Users assigned to the selected security level can view all documents, folders, and subfolders in Workflow Monitor.
Monitor documents limited	Users assigned to the selected security level can view only the documents, folders, and subfolders in Workflow Monitor to which they have read access.
None	Users assigned to the selected security level cannot open Workflow Monitor.

7. To save changes and close the window, click **Apply**.

Copying or Renaming Projects

Exigen Workflow allows you to copy one project to another. By doing so, you can quickly create a new project without having to recreate custom fields, tables, and settings. You can edit the copied project as needed.

To copy a project, proceed as follows:

1. In the **Project Builder** window, select the project and click **Copy**.



The **Copy Project** dialog appears.

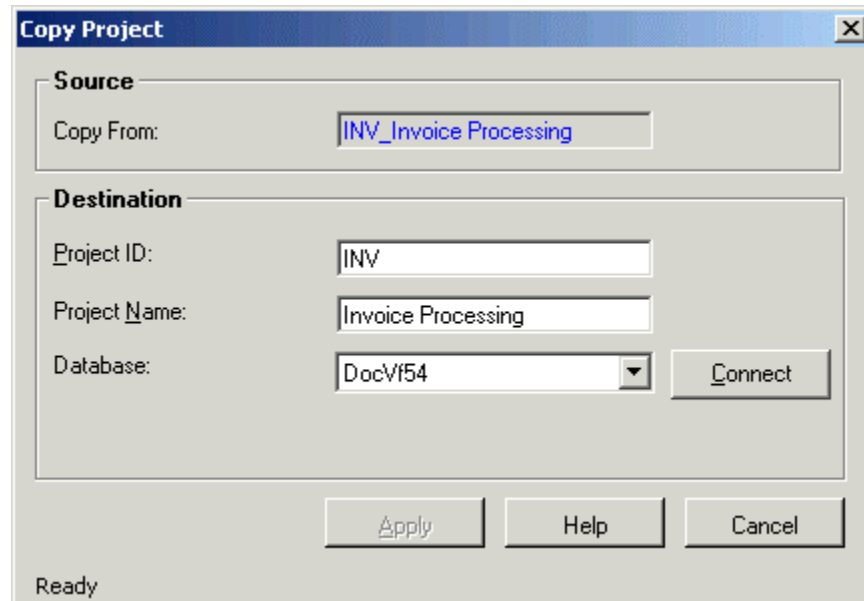


Figure 35: Copy Projects window

2. In the **Destination** section, enter the new project ID and name.
3. In the **Database** field, select the destination database for the new project.
For information on using a non-default database, see [Using a Non-Default Database](#).
4. To verify that the database connection is valid, click **Connect**.
5. To save your settings, click **Apply**.
6. To close the window without saving changes, click **Cancel**.
7. To open a help file, click **Help**.
8. Calculate the space and create the new project as described in [Creating a New Project](#).

The new database structure includes any custom tables and fields created in the original project.

9. Configure the project as described in [Configuring the Project](#).

To rename a project, proceed as follows:

1. Select the project and click **Modify Project**.



The **Modify Project** dialog appears.

Modify Project

Source

Project ID: INV

Rename From: INV_Invoice Processing

Destination

Project Name: Claim Processing

Apply

Cancel

Help

Figure 36: Modify Project

You can change only the project name.

2. Enter the new name and click **Apply**.
3. To close the window without saving changes, click **Cancel**.
4. To open a help file, click **Help**.

Exporting Projects

If the same project is to be used in a different Exigen Workflow database or outside your network setup, export files of your project tables and data can be created. This ensures that the new project is identical to the original one without requirement to re-enter customized data.

Exporting tables and table data are two separate functions. You do not have to export all the data in the database each time you export a project. Exporting data eliminates the need to re-enter data from the existing project into the new one.

The following topics are described in this section:

- [Exporting Tables](#)
- [Exporting Data](#)

Exporting Tables

To export only tables from a specific project, proceed as follows:

1. In the **Project Builder** window, select the project name.
2. Select **Project > Export Project > Tables**.

The **Export Project** window appears.

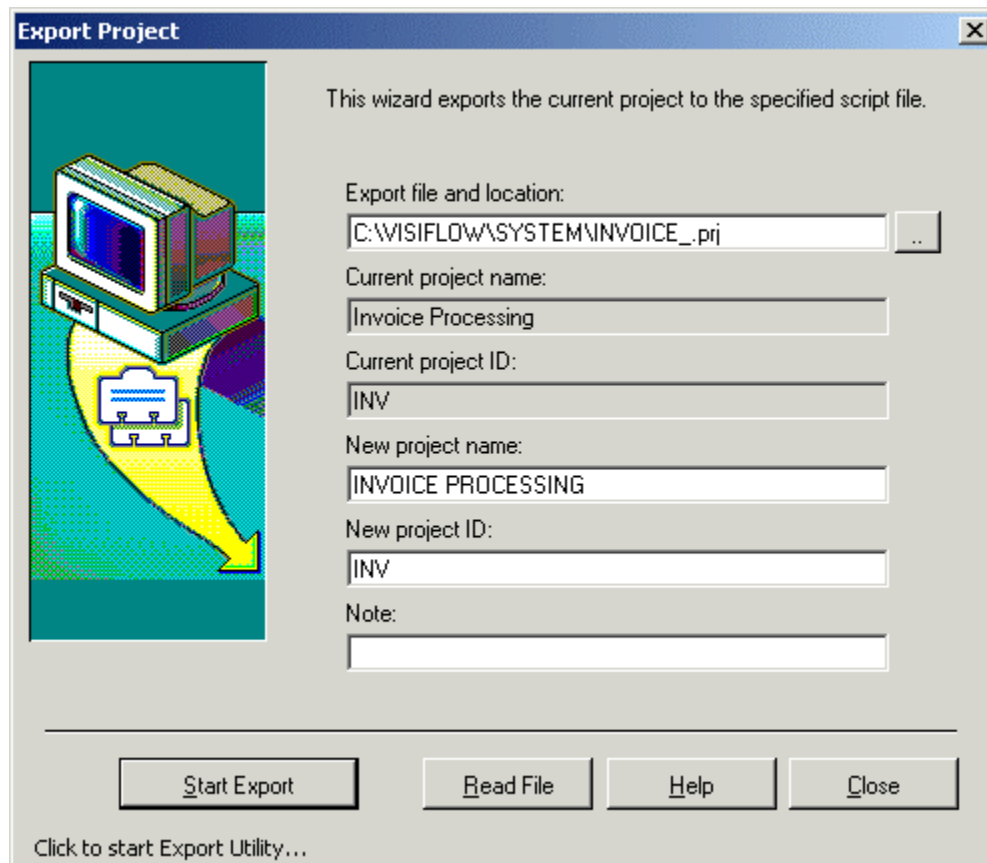


Figure 37: Export Projects window, exporting project tables

In the **Export file and location** field, the system inserts the path to the Exigen Workflow system directory and names the export file using the first 8 characters of the project name followed by a .PRJ extension. Note that spaces in a file name are replaced by an underscore.

3. To change the file path, click the browse button.
4. To change the export file name, enter a new value over the existing value. Ensure that the extension remains .PRJ.

The current project name and project ID are displayed in the next two fields.

In the **New project name** and **New project ID** fields, the same values appear automatically, but they can be changed if required.

5. In the **Note** field, enter any comments to be included with the export file.
6. To begin creating the export file, click **Start Export**.

During file creation, the buttons are disabled. When the creation process is completed, they are enabled again.

7. To view the exported file, click **Read File**.

The export project script is displayed using Notepad. The exported file can now be imported into another system.

Exporting Data

To export project data, proceed as follows:

1. Select the desired project.
2. Select **Project > Export Project > Data**.

The **Export Project Table Data** window appears.

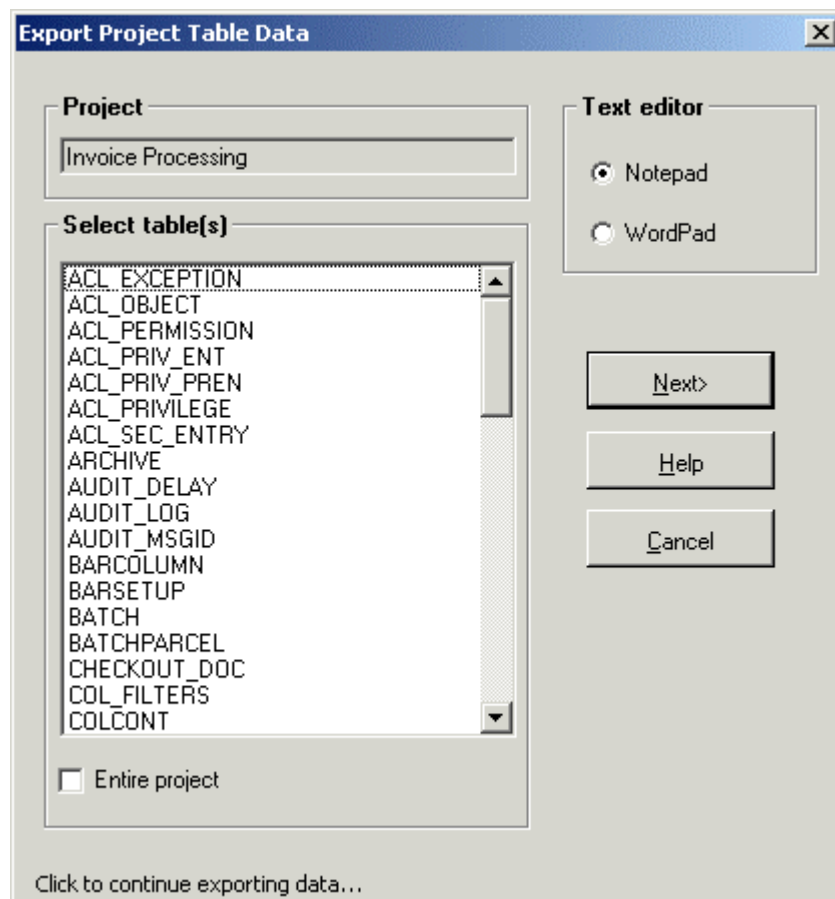


Figure 38: Export Project Table Data window, selecting project data for export

The project name is displayed at the top, with a list of all tables in the project beneath it.

3. To export the data from all project tables, select the **Entire project** check box. To export individual table data, select the corresponding table names.

Warning: Be careful when exporting the entire project at the same time. The resulting file can be very large. Ensure that there is sufficient space on the destination disk.

4. In the **Text editor** section, select whether you want the script file to be opened with Notepad or WordPad.

5. To proceed to the **Export Project Data** window, click **Next**.

The **Export Project Data** window appears.

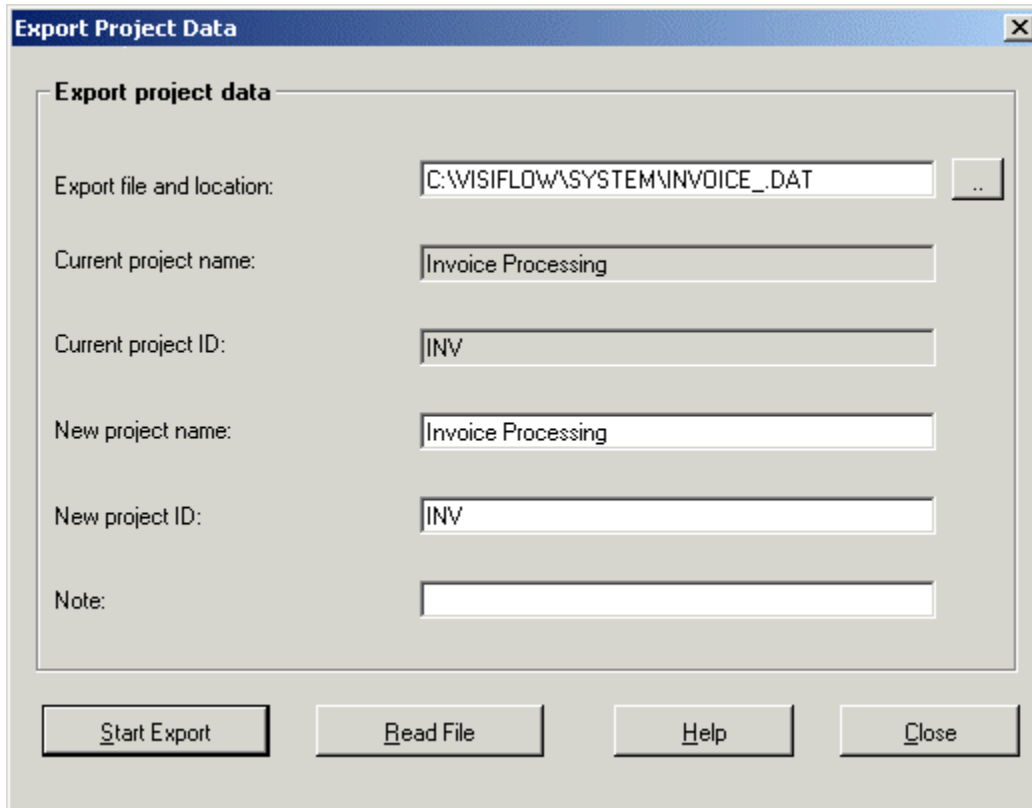


Figure 39: Export Project Data window

The export file name is generated with the path for the Exigen Workflow system directory and consists of the first 8 characters of the project name. The file extension is .DAT.

6. To change the export file name, click the browse button, or manually enter a different file name.

The **Current project name** and **Current project ID** are displayed as read-only fields.

7. If required, modify the **New project name** and **New project ID** fields.
8. In the **Note** field, enter comments associated with the project data.
9. After all values are entered, to create the new file, click **Start Export**.
10. When complete, to view the exported data, click **Read File**.
11. To return to the **Project Builder** window, click **Close**.

Importing Projects

To import a project, first import the tables, and then import the data. When you import a project, you are simultaneously creating it. Therefore, you do not need to have the new project listed in your **Project Builder** window. You must have at least one project already created in your system. In other words, you have previously entered a New Project name and ID, calculated the space, and created the project, but you did not have to make any custom tables or configure any settings. If the project being imported is the only one you are using, you can delete the existing project once the import is complete.

If you use a DB2 or Oracle database and import a project without using Project Builder, ensure that the tablespaces of the source and target projects match. If the tablespaces do not match, in the S00_PROJECT table, manually enter the target tablespace in the DBPASSWORD field.

The following topics are described in this section:

- [Importing Tables](#)
- [Importing Data](#)

Importing Tables

To import the project tables, proceed as follows:

1. Select **Project > Import Project > Tables**.

The **Import Project** window appears.

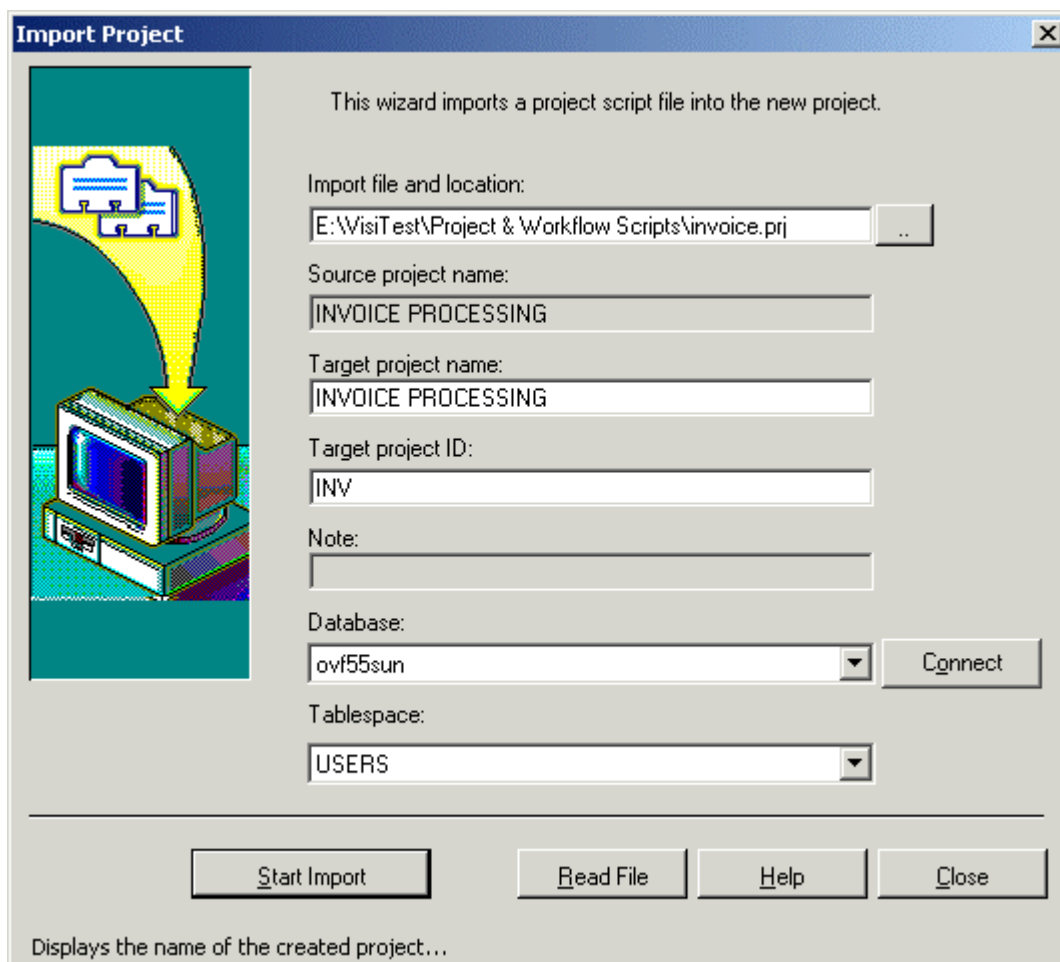


Figure 40: Import Project window, import project tables

2. To locate the import file path and file name, click the browse button.

When the import path is located, the remaining data is entered automatically.

The **Source project name** field displays the original project name.

The **Target project name**, **Target project ID**, and **Notes** values are entered during the export process.

The **Database name** corresponds to the database where the exported project was created.

All values except **Source project name** can be changed.

3. To verify the connection to the database, click **Connect**.
4. If an Oracle database is used, in the **Tablespace** field, select the tablespace.
5. To view the project file, click **Read File**.
6. When all values are correct, click **Start Import**.
7. When the import is complete, click **Close**.

The project is listed in the **Project Builder** window.

Importing Data

To import data from another project, proceed as follows:

1. Select **Project > Import Project > Data**.

The **Import Project Data** window appears.

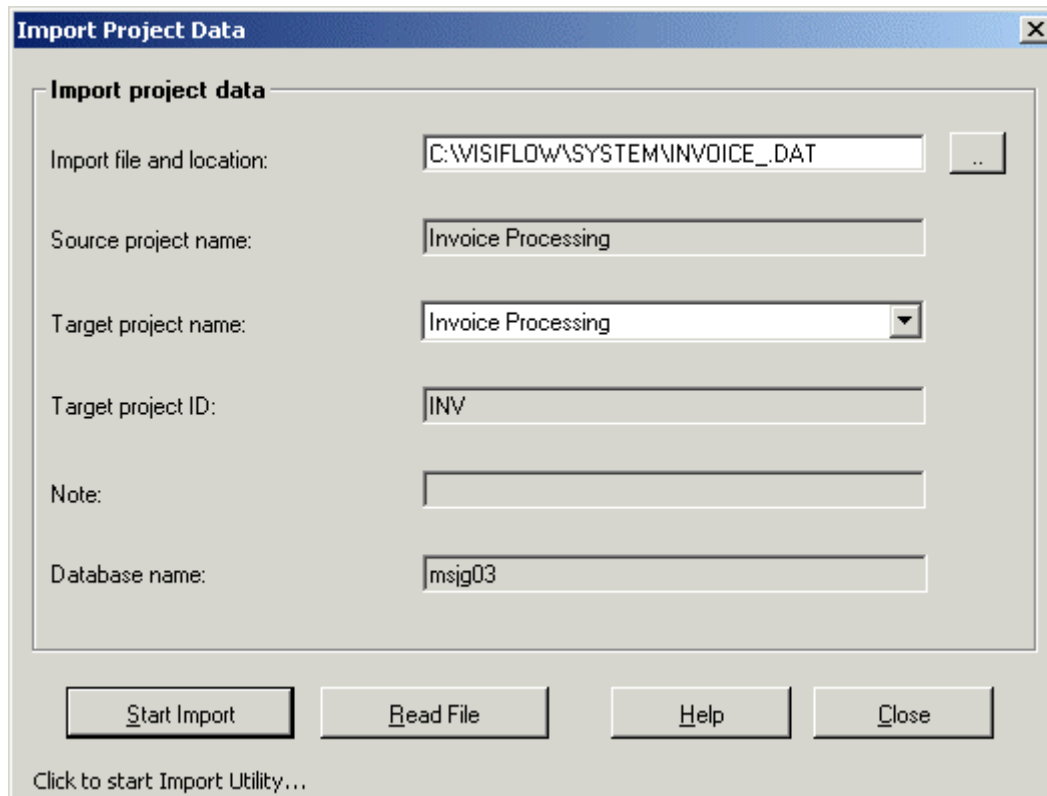


Figure 41: Import Project Data window

2. To locate the data file path and name, click the browse button next to the **Import file and location** field.

When the data file path and name are selected, the remaining fields are filled in automatically.

The **Source project name** field displays the project from which the data was exported.

The **Target project name**, **Target project ID**, and **Note** values are those assigned during the export process.

3. If the title listed is incorrect, search the **Target project name** list box to locate the project into which you are importing the data.
4. To view the project file, click **Read File**.
5. When all editable field values are entered, click **Start Import**.

If the source and target database brands differ, data records to be imported may exceed the maximum table column length in the target database. If this occurs, a confirmation dialog appears.

6. To import all data records and truncate those exceeding maximum length, click **Yes**.
7. To import the data records that do not exceed maximum length and skip data records that exceed the maximum length, click **No**.
8. To complete the import process, click **Close**.
9. Configure the project as described in [Configuring the Project](#).

Checking the Project Version

Exigen Workflow version upgrade releases typically include additions or changes to the tables and table structures. In such cases, it is necessary to ensure database integrity by synchronizing the existing project database table structures with the table structures in the new releases.

The **Check Project Version** feature in Project Builder performs this function. If there are multiple projects in the system, each project must be checked.

To synchronize a project with any changes, proceed as follows:

1. In Project Builder, select the project.
2. Select **Project > Check Project Version** or press **F8**.

If an Oracle, DB2 z/OS, or DB2 AIX database is used and a tablespace for the project is not specified, the **Server** window appears and displays available tablespaces.

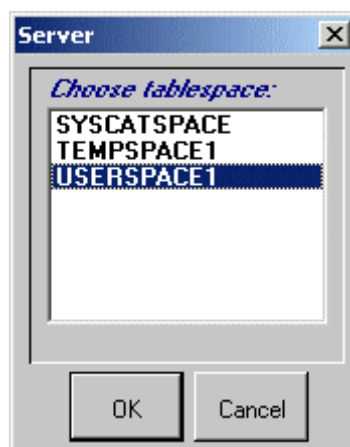


Figure 42: Server window with available tablespaces

3. If the **Server** window appears, select a tablespace for the project and click **OK**.

The **Check Project Version** window appears and automatically begins checking the database.

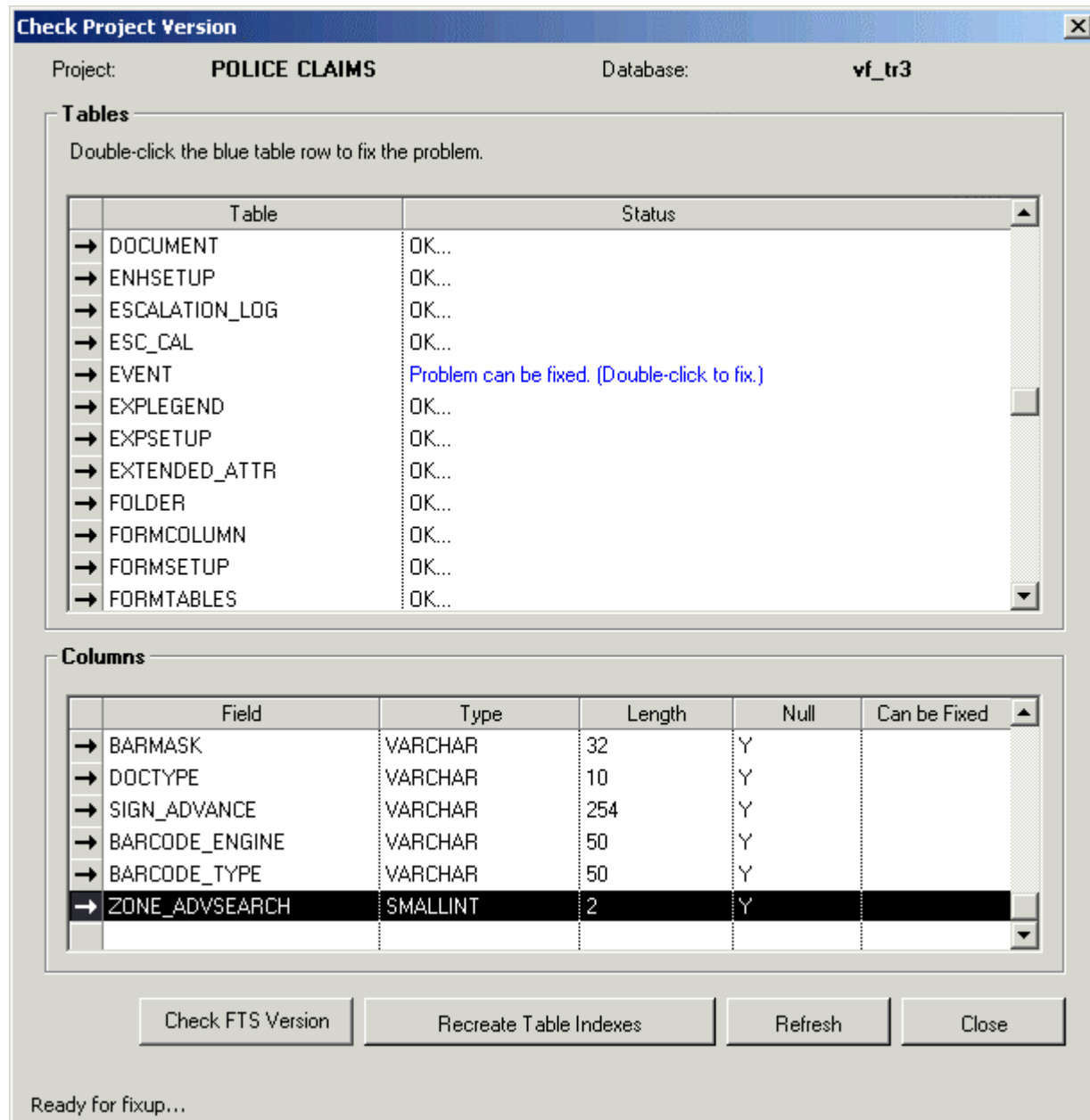


Figure 43: Checking project tables

If an audit project is selected, Project Builder automatically starts deploying audit event descriptions by running the `500audit.sql` script file, which adds records to the audit project's `AUDIT_MSGID` table.

The name of the project that is checked and the database where the project is located are displayed at the top of the window. Each table is displayed in a list once the fields are checked. The fields are listed in a separate table in the lower part of the window. The status of each table is displayed next to the table name once it is checked. The normal status is **OK**.

If there is a discrepancy between the existing structure and the new structure of a table, one of the following statuses are displayed in the **Status** column:

Project table discrepancy statuses	
Status	Description
Problem can be fixed	Some columns are missing or existing columns must be modified in the table.
Missing table	A project table is missing.
Unique index problem	A system index in the SUBFOLDER table does not include all required columns. The set of columns that must be included in the index depends on the current project indexing scheme.
Problem cannot be fixed	There is a problem in the database table that cannot be automatically fixed by Project Builder. To fix this problem, contact Exigen Support Services.

4. To correct a discrepancy and change the status to **OK**, double click the status.

Sometimes fixing a problem requires creating a temporary database table. In this case, a warning message is displayed.

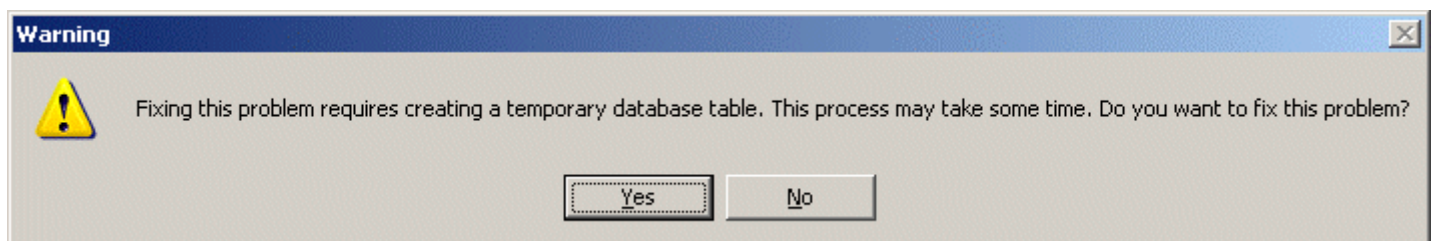


Figure 44: Warning message when fixing a problem requires creating a temporary database table

Fixing a problem that requires creating a temporary database table may take some time.

5. If the warning message appears, perform one of the following steps:
 - To fix the problem, click **Yes**.
 - To postpone the database update for this problem, click **No**.
6. Repeat the steps in this procedure until all table discrepancies are corrected.
7. To perform a version check for FTS tables, click **Check FTS Version**.
8. When all tables are checked, rebuild table indexes by clicking **Recreate Table Indexes**.

This deletes all existing system indexes and recreates them. Indexes can be rebuilt for only one table at a time.

If Project Builder cannot fix a problem, the administrator must contact Exigen Support Services.

Full Text Search

The **Full Text Search** feature searches for documents based on text contained in the documents. Full Text Search uses optical character recognition (OCR) to identify words and phrases within documents. These words or phrases can be used to locate specific documents within the database.

To add Full Text Search to a project, proceed as follows:

1. Open the **Project Table Maintenance** window.
2. Select **Maintenance > Create FTS Tables**.

FT appears under the database type field in the **Project Table Maintenance** window.

If you are making an existing project searchable by FTS, documents created before FTS implementation cannot be located using FTS because they were not subject to OCR when they entered the system.

To delete Full Text Search from a project, proceed as follows:

1. Open the **Project Table Maintenance** window.
2. Select **Maintenance > Drop FTS Tables**.

You can also access the Drop FTS feature from the **Project** menu in the **Project Builder** window.

Unique and Cluster Indexes

When Exigen Workflow is installed and a project is created, internal indexes are created on specific tables to enhance system performance. Because custom tables and fields are not added until after your project is created, indexes cannot be created for them until later. This must be done manually.

The following topics are described in this section:

- [Unique Indexes](#)
- [Cluster Indexes](#)

Unique Indexes

When you set up custom fields, one of the attributes determines if the field is to be part of the **unique** index. All fields with this attribute set to **Yes** on a specific table are used to create a unique index for that table. Note that only the combination of these fields can create a unique index, not an index for each individual field.

Warning: The Folder table must contain at least one index field. It is not created automatically. You must add it manually.

To create a unique index on the selected table, proceed as follows:

1. In the **Project Table Maintenance** window, select **Maintenance > Create Unique Index**.
2. To drop the index, select **Maintenance > Drop Unique Index**.

If you add a new unique field to your table, you must first drop the current index before creating a new one.

Cluster Indexes

Cluster indexes combine similar data in certain areas of the database. Exigen Workflow cluster indexes are driven by the FLD_RSN field value. A folder number is assigned to each record. Because documents and parcels also include a folder number as part of the record, they are stored together with the folder in the database.

The limitation in using cluster indexes in Exigen Workflow is that you can only use them if indexing is part of the main workflow. This is because when documents and parcels are scanned into the system, a folder number of 999999999 is automatically assigned. It is not until the parcels and documents are indexed that they are given a valid folder number. Cluster indexes cannot work properly without a valid folder number.

If your system uses a separate project and database for the scanning and indexing process and the parcels and documents are exported to a different project and database, cluster indexes must be created in the export project to enhance system performance.

To create cluster indexes, proceed as follows:

1. In the **Project Table Maintenance** window, select **Maintenance > Create Cluster Indexes**.
2. To drop the cluster indexes, select **Maintenance > Drop Cluster Indexes** menu item.

Advanced Features

You can customize certain Exigen Workflow functions by making additions to the project tables in the database. The addition of certain fields and tables automatically triggers a set of features otherwise unavailable in a standard Exigen Workflow installation.

Using an Oracle Database with Synonyms

Exigen Workflow provides limited support of configurations where database tables, views, and sequences are accessed using Oracle synonyms. Synonyms are useful when the database user that is used to connect to the database cannot be the owner of Exigen Workflow tables, views, and sequences.

To create a project that uses synonyms, proceed as follows:

1. Create the Exigen Workflow database structure using the ID and password of the user who is the owner of Exigen Workflow tables, views, and sequences as described in *Exigen Workflow Installation Guide*, Chapter 2: Installing Exigen Workflow, Creating or Upgrading the Exigen Workflow Database Structure.
2. Create and configure the project as appropriate.
3. Create synonyms for Exigen Workflow tables, views, and sequences.

Exigen Workflow project tables, views, and sequences are named according to the following naming convention rules:

- The first three letters are the project ID.
- The project ID is followed by an underscore and the table or view name, for example, *INV_DOCUMENT*.
- Sequences have additional characters *_SEQ_* after the project ID, for example *INV_SEQ_DOCUMENT*.

Exigen Workflow master database tables are named as follows:

<prefix>_<combination of characters>

The following table prefixes are reserved:

- EIS
- U00
- VML
- Sxx
- Wxx

where xx is a number from 00 to 30.

Master Exigen Workflow database views are named as follows:

SYS<arbitrary name>_DTM

An example of a master Exigen Workflow database view name is *SYSIND_COL_DTM*.

4. Open the *VISI.INI* file for editing.
5. In the *[databases]* section, locate the appropriate *DBS_MASTER* record and configure the *DBS_USER* and *DBS_PASSWORD* parameters as follows:

DBS_USER=<user ID>

DBS_PASSWORD=<password>

where *<user ID>* and *<password>* define the user who is used to connect to the database.

6. Save and close the *VISI.INI* file.

The following limitations apply:

- Workflow DB Startup and Project Builder cannot create and modify database objects that are not owned by the user specified in the *VISI.INI* file.

To perform these tasks, the database user who is used to connect to the database must be the owner of the Exigen Workflow tables, views, and sequences. To run Workflow DB Startup or Project Builder, the *DBS_USER* and *DBS_PASSWORD* parameter values in the *VISI.INI* file must be changed to specify the owner of the database objects.

- Synonyms are not created automatically.

If a new database table, view, or sequence is created, the appropriate synonym must be created for it manually.

Chapter 4: Setting Up Exigen Workflow

The following topics are described in this section:

- [Overview](#)
- [Setting Up the System](#)
- [Using the System Setup Window](#)
- [Maintaining Project Tables](#)
- [Maintaining Storage Locations](#)
- [Scheduling Activities](#)
- [Setting Up Document Access Control](#)
- [Setting Up and Printing Reports](#)
- [Viewing and Modifying Configurations](#)
- [Setting Up Folder History Browsing](#)
- [Specifying Scanner Specific Settings](#)

Overview

Before you start the administrative process, you must have a project. For information on setting up projects, see Chapter 3: Creating Projects.

Setting up the system is the first step in Exigen Workflow administration. The setup consists mainly of setting up security and basic Exigen Workflow options. When you set up Exigen Workflow, you establish the basic rules from which Exigen Workflow and the workflow derive their information.

The following setup procedures are performed before users can access the system:

Setup procedures		
Procedure	Description	Required during setup
Specifying security levels	Specifies security level access rights to Exigen Workflow applications and objects.	Yes.
Specifying access levels	Specifies security restrictions on folders and subfolders.	Recommended.
Setting up corporate locations	Specifies user locations.	No.
Setting up users	Maintains user access rights and defines user IDs, passwords, security levels, document access rights, and other attributes.	Yes.
Setting up	Groups users by department or function and provides access	Recommended.

Setup procedures		
Procedure	Description	Required during setup
workflow groups	to workflow objects.	
Setting up a workflow	Creates workflow nodes and the links between them.	Yes.
Setting up tasks	Sets up task objects, which are external applications such as Word.	No.
Setting up events	Sets up automatic processes performed by Automatic Queue Server. In previous Exigen Workflow versions, events were processed by Advanced Event Server. In the current Exigen Workflow version, Automatic Queue Server handlers can be set up to process events.	No.
Managing stamps	Defines user rights for applying electronic rubber stamps to images.	No.
Setting up locations	Defines storage locations for workflow scripts, form templates, and electronic rubber stamps.	No.
Setting up global user groups	Defines global user groups to specify access to documents and document annotations.	No.
Setting up document context security levels	Specifies document access levels for global user groups. For example, a particular global user group can be granted the right to view, modify, and delete electronic posted notes attached to documents.	No.
Maintaining project tables	Sets up folders, subfolders, and document types.	Yes.

In addition, Exigen Workflow can be integrated with Exigen E-Mail. Exigen Workflow integration with Exigen E-Mail enables users to send Exigen E-Mail documents to Exigen Workflow and import them as documents in parcels. After successful integration, Exigen E-Mail documents can be accessed and viewed in Exigen Workflow.

Note: Exigen E-Mail settings are specified in the **Administrator** window. For information on Exigen E-Mail settings, see the *Exigen Workflow Installation Guide*, Chapter 5: Integrating Exigen Workflow with Other Exigen Products, Integrating Exigen Workflow with Exigen E-Mail.

All setup procedures, except maintaining project tables, relate to all projects in your Exigen Workflow system. Setup procedures for maintaining project tables relate to only one project at a time. You must only define a user once, and not for every new project. If you add a user to a certain workflow group, this user can use any node in any workflow that can be accessed by that group.

Setting Up the System

The Administrator tool is used to set up the system. The Administrator tool is located in the **Workflow Tools** folder in **Administration Tools** in Exigen Workflow Explorer. The icon appears as follows:



When it is clicked, the **Administrator Utilities** window appears.

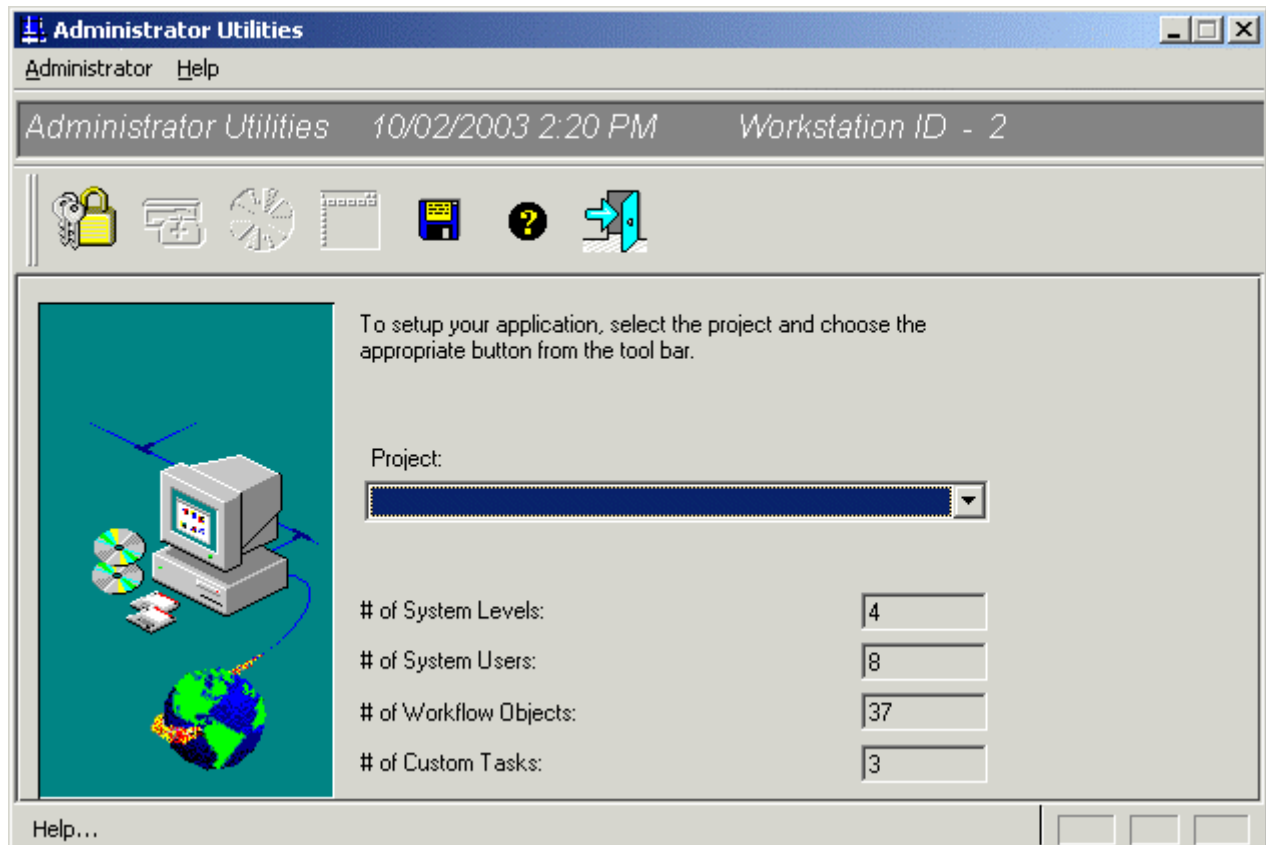


Figure 45: Administrator Utilities window

The fields under the **Project** list display the following basic attributes of the entire Exigen Workflow system:

- number of system levels
- users
- workflow objects
- custom tasks

To specify system settings such as the following, click **System Setup**:

- security levels

- access levels
- corporate locations
- users
- workflow groups
- workflow objects
- tasks
- events
- stamps
- global user groups
- document context security levels

Several users can work with Administrator simultaneously if they are working in different functional areas. If a user is trying to open an Administrator tool that is being used by another user, a warning message is displayed and the tool is not available. For example, User A configures project settings, and User B configures workflow events. User C cannot configure project settings or workflow events, but is able to configure user groups.

The **System Setup** window appears. For information on setup, see [Using the System Setup Window](#).

To specify the project configuration, optical disc configuration or project tables, proceed as follows:

1. In the **Project** list, select a project.

The **Project Configuration**, **Optical Disc Utilities**, and **Table Maintenance** toolbar buttons are enabled.

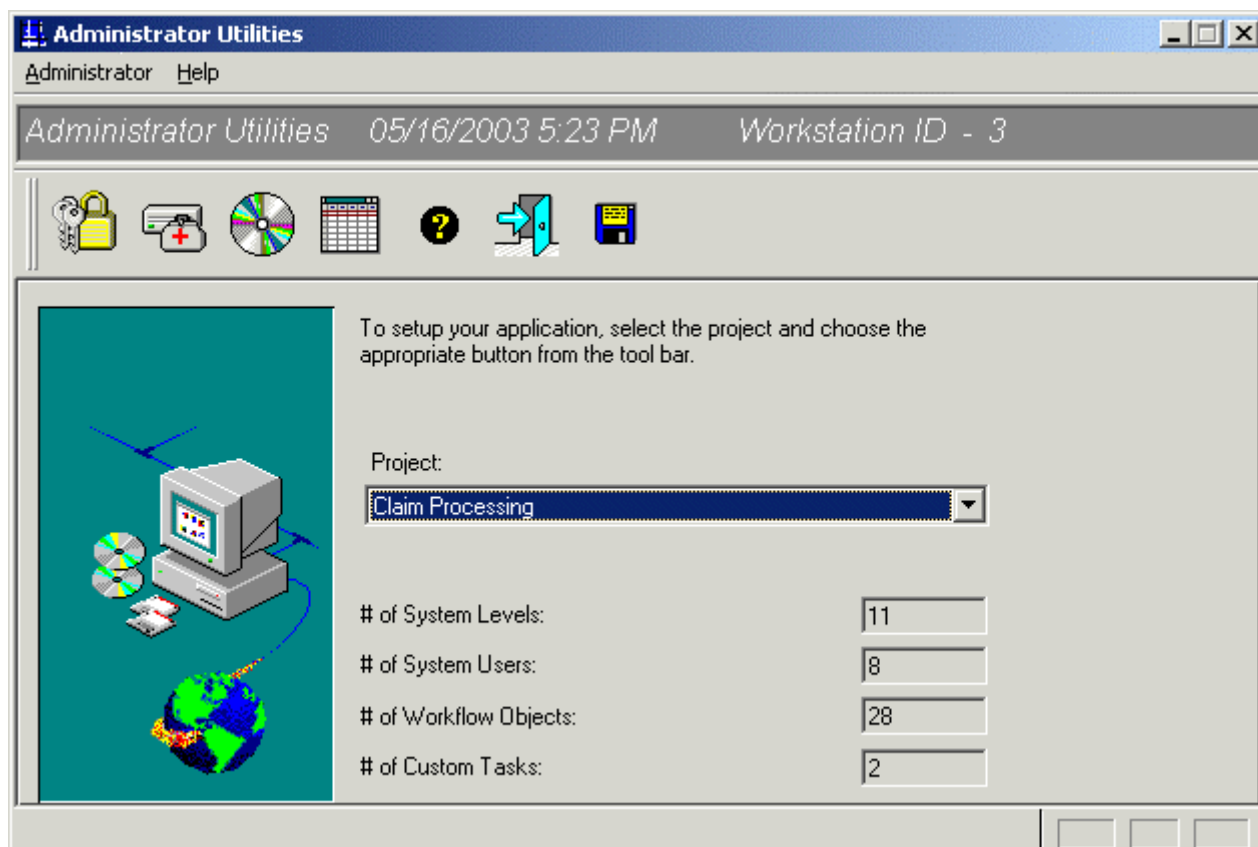


Figure 46: Administrator Utilities window with a selected project

Every new Exigen Workflow project that you create contains three default users:

- regular user DTM
- common user COM
- common user FIX

By default they are assigned the only predefined security level: Administrator.

2. To open the **Project Configuration** window, click **Project Configuration**.



For more information on project configuration, see [Configuring the Project](#).

3. To ensure that the **Administrator Utilities** window is displayed at the same position next time it is opened, click **Save Configuration**.



4. To close the **Administrator Utilities** window, click **Exit**.



Specifying Security Settings

To specify password settings in your system, proceed as follows:

1. In the **Administrator Utilities** window, select **Administrator > Security Settings**.

The **Security settings** window appears.

Security Settings

Name: Default

Password settings

Min. password size: 1

Min. days between password changes: 0

Max. days between password changes: 0

Min. number of digits in password: 0

Min. number of symbols in password: 0

Min. number of uppercase letters: 0

Min. number of lowercase letters: 0

Max. login retries before locking out login: 0

Number of previous passwords to remember: 0

Password lock time (DD-HH:MM): 00-00:00

Number of inactive days after which account is disabled:

Number of inactive days after which account is deleted:

Days before password expiration for displaying warning:

☐ Hash passwords

☐ Prohibit multiple logins using the same login name

☒ Enable users to create shortcuts from Workflow Explorer

OK Help Cancel

Figure 47: Security settings window

2. To specify the minimum and maximum number of days between password changes, enter values in the **Min. days between password changes** and **Max. days between password changes** fields.

If the maximum number of days is set to 0, the password does not expire.

3. In the appropriate fields, enter the following minimum values for the password:

- password size
- number of digits
- symbols
- uppercase letters
- lowercase letters

Note: All non-alphanumeric characters are considered symbols.

4. To specify the maximum number of login attempts, in the **Max. login retries before locking out login** field, enter a value.

If a user attempts unsuccessfully to log in more times than is specified in this field, the login is locked for a period of time specified in the **Password lock time** field.

If the number is set to 0, the user is never locked.

5. To limit reusing passwords, in the **Number of previous passwords to remember** field, enter a value.

The number defines how many passwords are saved in the password history to prevent reusing previous passwords. This number also includes the current password, so caution must be exercised when setting it. If the user exceeds the set number of failed login attempts, the user login is locked out automatically.

6. To specify the length of time for locking out a user, in the **Password lock time** field, enter a value.

If the time is set to 00-00:00, the user is never locked.

7. To specify the number of days before a user account is disabled if the user performs no actions, in the **Number of inactive days after which account is disabled** field, enter the number.

8. To specify the number of days before a user account is deleted if the user performs no actions, in the **Number of inactive days after which account is deleted** field, enter the number.

9. In the **Days before password expiration for displaying warning** field, specify how many days before the password is expired a user receives a warning.

10. To instruct the system to store the password in the encrypted format, select **Hash passwords**.

The system administrator cannot see the hashed password. Hashed passwords increase security if the same passwords are used in different systems.

Password length depends on the password hashing setting. Effective password length is limited to 32 bytes, not characters, when password hashing is disabled. Users or administrators can enter longer passwords in non-hashed mode, but only the first 32 bytes of the password are used. In hashed password mode, passwords can have an arbitrary length.

11. To prevent simultaneous work sessions using the same user ID and password, select **Prohibit multiple logins using the same login name**.

12. To allow users to create Exigen Workflow shortcuts on the desktop, select **Enable users to create shortcuts from Exigen Workflow Explorer**.

The shortcuts contain security information such as user ID and password.

13. To decrease the risk of unauthorized access to the system, clear the **Enable users to create shortcuts from Exigen Workflow Explorer** option.
14. To save changes, click **OK**.

Note: All users must log in again to enable shortcut changes.

Specifying Audit and Reconnection Settings

The **Audit Setup** window is used to specify global audit and reconnection settings for the Exigen Workflow system.

To specify audit and reconnection settings, proceed as follows:

1. Select **Administrator > Audit Setup**.

The **Audit Setup** window appears.

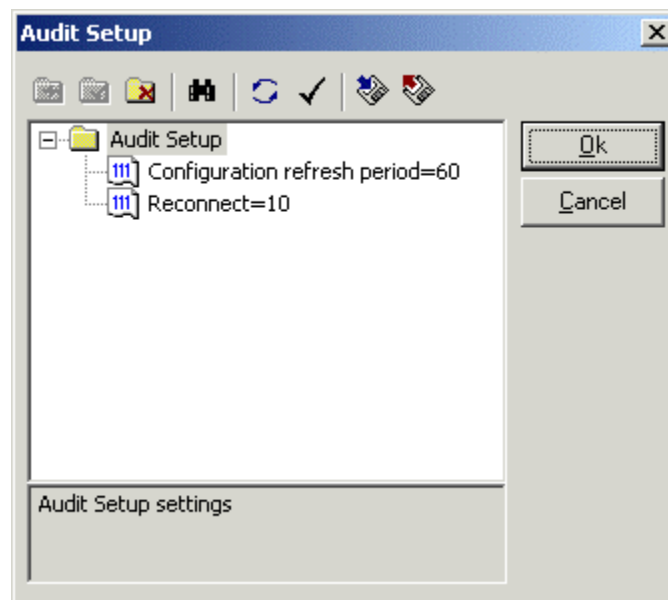


Figure 48: Specifying audit settings

The **Configuration refresh period** option is used to specify the interval in minutes after which audit filters are refreshed. For information on audit filters, see [Defining Audit Filters](#).

2. To modify the refresh value, right click **Configuration refresh period** and select **Edit**.
3. In the **Configuration refresh period** field, enter a value.

Configuration refresh period values are described in the following table:

Configuration refresh period values	
Value	Description
0	Turns off the audit filter refresh function. It improves Exigen Workflow

Configuration refresh period values	
Value	Description
	performance.
60	Refreshes audit filters every 60 minutes. This is the default value.
> 60	Refreshes audit filters at specified intervals. It improves Exigen Workflow performance.

The **Reconnect** option is used to specify the delay in minutes before a reconnection attempt is made if the connection to the Exigen Workflow database is lost.

- To modify the reconnection value, right click **Reconnect** and select **Edit**.
- In the **Reconnect** field, enter a value.

Reconnection values are described in the following table:

Reconnection values	
Value	Description
0	Turns off the reconnection function. If the connection to the Exigen Workflow database is lost, no attempt is made to automatically restore it.
10	Reconnection is attempted 10 minutes after the database connection is lost. This is the default value.
Other positive value	Reconnection is attempted at the specified interval.

- To cancel changes and close the window, click **Cancel**.
- To save changes and close the window, click **Ok**.

Defining Audit Filters

To define audit data collected in your system, select **Administrator > Audit Filters**.

The **Audit Filters** window appears.

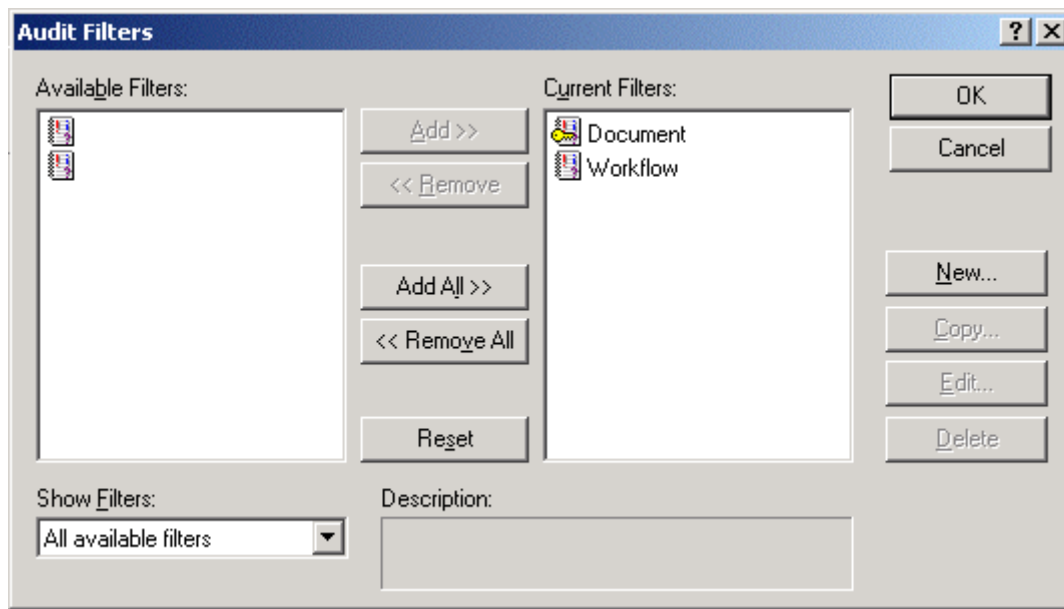


Figure 49: Audit Filters

This window shows the available filters and current filters. The first time it is used, this window displays the default filters in the current filters list if you answered **Yes** to the system warning about active audit filters when an audit project is created. You must change these defaults to use auditing in your system.

An including or excluding filter can be used. For more information on including and excluding filters, see [Creating Filters](#).

The following tasks are available in this window:

- [Activating Filters](#)
- [Applying Activated Filters](#)
- [Creating Filters](#)
- [Copying Filters](#)
- [Editing Filter Definitions](#)
- [Deleting Filters](#)

Activating Filters

To activate an available filter, select it in the available filters list and click **Add>>**. The filter appears in the current filter list.

To activate all filters, click **Add All**.

To deactivate a filter in the current list, select it in the list and click **Remove**.

To deactivate all filters in the current list, click **Remove All**.

To cancel all changes and reset to the initial filter list of current filters in the **Audit Filter** window, click **Reset**.

Applying Activated Filters

To apply activated audit filters, proceed as follows:

1. Start Audit Server.
2. Click **Process Setup** or select **Run > Process Setup**.
3. In the **Audit Processing Settings** dialog, select **Use Audit Event Filters**.
4. Click **OK**.

Creating Filters

To create filters, proceed as follows:

1. Click **New**.

The **Edit Audit Filter** window appears.

The screenshot shows the 'Edit Audit Filter' dialog box with the 'Properties' tab selected. The dialog has a title bar with a question mark and a close button. Inside, there are two tabs: 'Properties' and 'Advanced'. The 'Properties' tab contains the following fields and controls:

- Name:** A text input field.
- Description:** A text input field.
- Public filter:** A checkbox.
- Excluding filter:** A checkbox.
- Event Class:** A dropdown menu with '<Any event class>' selected.
- Event Type:** A dropdown menu with '<Any event type>' selected.
- Event Message:** A dropdown menu with '<Any event message>' selected.
- Severity:** A spinner control.
- Event Phase:** A dropdown menu with '<Any event phase>' selected.
- Transaction:** A text input field.
- Date and Time:** A section containing:
 - From:** A dropdown menu with 'First Event' selected, followed by date and time pickers set to '6/ 7/2002' and '12:30:13 PM'.
 - To:** A dropdown menu with 'Last Event' selected, followed by date and time pickers set to '6/ 7/2002' and '12:30:13 PM'.
 - Use server time:** A checkbox.

At the bottom of the dialog are 'OK' and 'Cancel' buttons.

Figure 50: Edit Audit Filter, Properties tab

2. In the **Properties** tab, specify the following general filter properties:

- Enter a name that is unique and descriptive.
- Enter a description.
- To allow all users to view the filter, select the **Public** check box.

Only users with Administrator access rights can modify the filter. If the **Public** check box is cleared, the filter is visible only to the user who created it.

- To create an excluding filter, select the **Excluding filter** check box.
- In the respective boxes, select event class, type, message, and severity.

The **Transaction** field is for future use.

3. To specify advanced filter properties, select the **Advanced** tab.

Figure 51: Edit Filters window, Advanced tab

4. In the **System** area, specify settings for the system.
5. In the **Workflow** area, specify settings for the workflow.
6. In the **Project** area, specify settings for the project.
7. To save the settings, click **OK**.

Copying Filters

To create a filter based on an existing filter, proceed as follows:

1. Select a filter.
2. Click **Copy**.

The selected filter appears in the **Edit Filter** window.

3. Specify a name and change the corresponding settings.
4. To save the changes, click **OK**.

Editing Filter Definitions

To change the filter definition, proceed as follows:

1. Select the filter.
2. Click **Edit**.

The filter appears in the **Edit Filter** window.

3. Change the settings as required.
4. To save the changes, click **OK**.

Deleting Filters

To delete a filter, select it and click **Delete**.

To view audit data, select **Audit Viewer** in **Workflow Tools**. For information on using the Audit Viewer, see [Chapter 11: Using Audit Log Viewer](#).

For information on the Exigen Workflow auditing system, see [Appendix D: Audit Data in Exigen Workflow](#).

Configuring Document and Page Notes

For security reasons, administrators can disable the **Delete** button in the **Document Notes** and **Page Notes** windows in Image Viewer. **Delete** allows users to delete document and page notes. By default, it is disabled.

The status of **Delete** is defined in the `visiclt.ini` file located in the Windows directory.

To configure the status of **Delete**, proceed as follows:

1. Open the `visiclt.ini` file.
2. In the `[setup_view_settings]` section, perform one of the following tasks as required:
 - To enable **Delete**, modify the `DeleteNotes` parameter as follows:
`DeleteNotes=ON`
 - To disable **Delete**, modify the `DeleteNotes` parameter as follows:
`DeleteNotes=OFF`
3. Save and close the `visiclt.ini` file.

Using the System Setup Window

To open the **System Setup** window, in the **Administrator Utilities** window, click **System Setup**.



The **System Setup** window appears.



Figure 52: System Setup window

The buttons across the top of the **System Setup** window represent the first steps to setting up the system. The following topics are described in this section:

- [Specifying Security Levels](#)
- [Specifying Access Levels](#)
- [Setting Up Workflow Objects](#)
- [Setting Up Workflow Groups](#)
- [Setting Up Corporate Locations](#)
- [Setting Up Users](#)
- [Setting Up Tasks](#)
- [Setting Up Events](#)
- [Managing Stamps](#)
- [Setting Up Locations](#)
- [Setting Up Global User Groups](#)
- [Setting Up Document Context Security Levels](#)
- [Setting Up Document Types](#)
- [Setting Up Skills](#)
- [Setting Up and Using Annotation Security](#)

Specifying Security Levels

Security Level setup combines both system access and workflow object authorization. Each user must be assigned a security level.

Setting up security levels consists of the following two main steps:

- defining which applications each security level can access

- defining which workflow objects each security level can access and which operations can be performed within each object

To set up security levels, proceed as follows:

- Click **Security Level Setup**.



The **Security Level Setup** window appears.

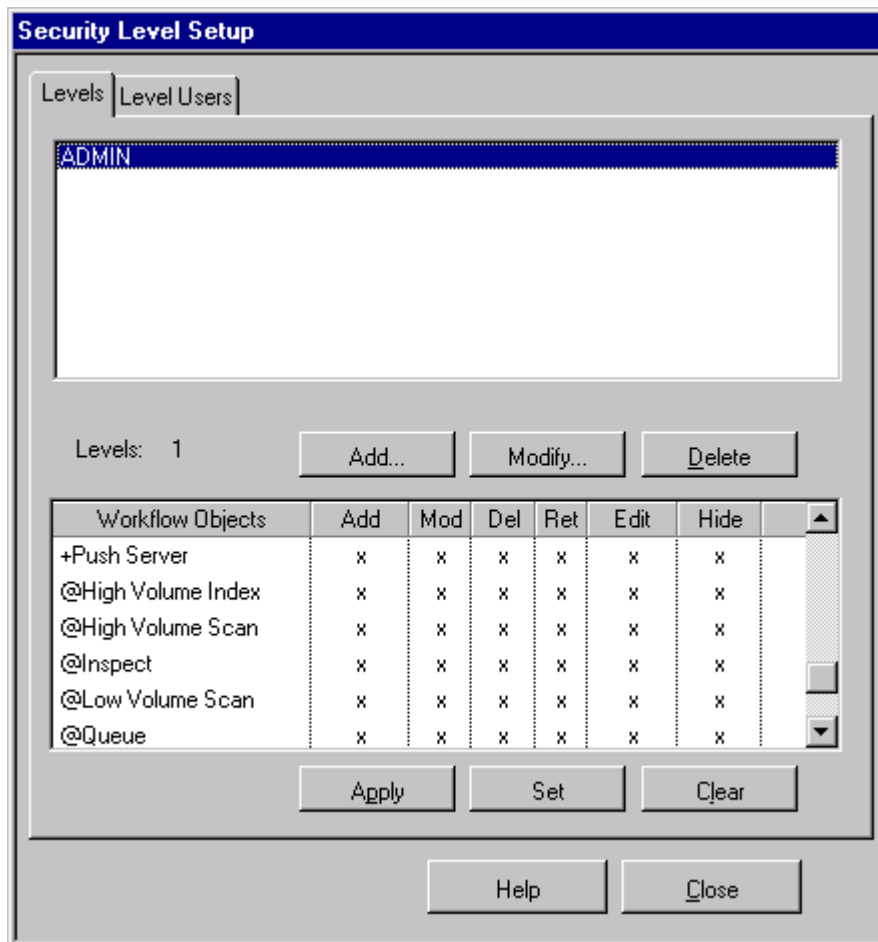


Figure 53: Security Level Setup window

The **Levels** tab lists all security levels in the system. For more information on the **Security Level Setup** dialog, see [Security Level Setup Dialog](#).

- To view all users assigned to the selected level, select the **Level Users** tab.

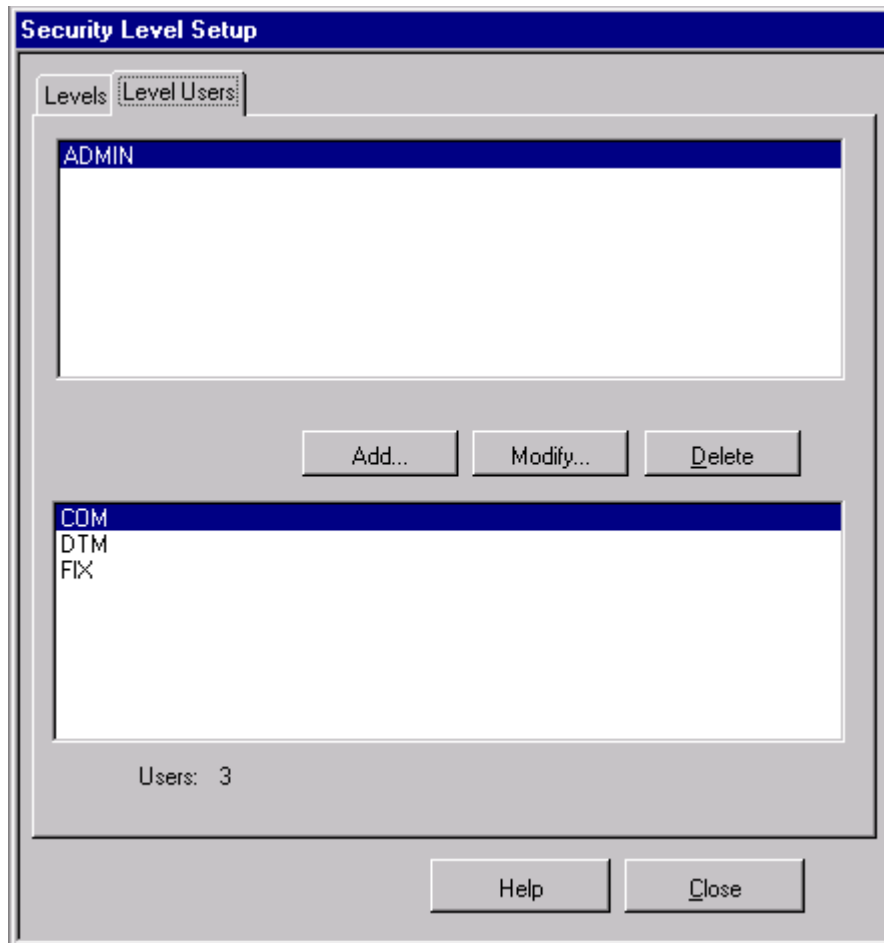


Figure 54: Security Level Setup, Level Users tab

Note: Users cannot be added to or removed from the list in the **Security Level Setup** window. For information on adding or removing users, see [Setting Up Users](#).

3. To add a new security level, click **Add**.

The **Add Level** dialog appears. For information on the **Add Level** dialog, see [Add Level Dialog](#).

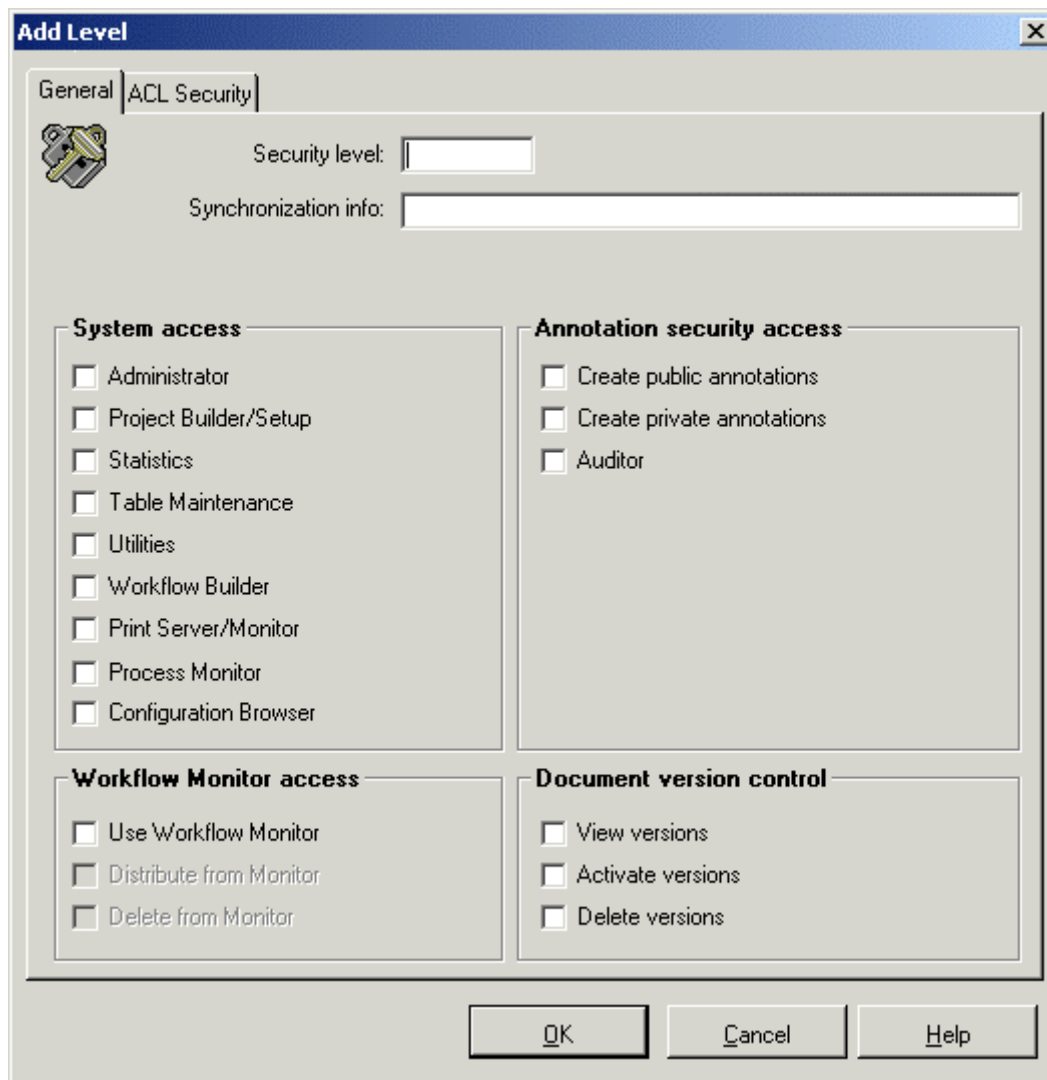


Figure 55: Add Level window

4. If the project is configured to use ACL based security, in the **ACL Security** tab, configure the settings as described in [Specifying the Security Settings for a Security Level](#).
5. In the **Security level** field, enter the name of the new security level.
6. To use NT and Exigen Workflow user synchronization, in the **Synchronization info** field, enter the name of a Windows NT® workgroup or the path to the directory.

For more information on synchronization, see [Chapter 10: Setting Up User Synchronization Service](#).

7. In the **Database role** field, select the appropriate database role.

For information on database roles, see [Add Level Dialog](#).

8. To provide users with access to features, in the **System access** section, select the appropriate feature as described in the following table:

System access features	
Feature	Description
Administrator	<p>Administrator utilities such as the following:</p> <ul style="list-style-type: none"> • system setup • project configuration • optical functions <p>This feature also grants access to Audit Viewer, Users Synchronization Setup, and the SQL Talk utility, which allows users to modify the Exigen Workflow database by writing SQL statements.</p> <p>SQL Talk is not available if it is disabled in the <code>visiclt.ini</code> file located in the Windows directory.</p> <p>In the <code>visiclt.ini</code> file, the status of SQL Talk is defined by the <code>sql_talk</code> parameter in the <code>[setup_system_access]</code> section as follows:</p> <ul style="list-style-type: none"> • If the Administrator option is selected and the value of the <code>sql_talk</code> parameter is set to 1, SQL Talk is available to users with the defined security level. • If the value of the <code>sql_talk</code> parameter is set to 0, SQL Talk is not available to users even if the Administrator option is selected in the security level setup.
Project Builder/Setup	Project Builder application and Configuration function.
Statistics	Statistics application.
Table Maintenance	Administrator utility and table maintenance function.
Utilities	Workflow Viewer, Exigen Workflow database, and image utilities listed in Utilities folder in Administration Tools in Exigen Workflow Explorer.
Workflow Builder	Workflow Builder, Workflow Viewer, Component Configuration Manager, and E-Capture Administrator.
Print Server/Monitor	Print Server and Print Monitor applications.
Process Monitor	Process Monitor application.
Configuration Browser	Configuration Browser application.

The **Workflow Monitor access** section displays options that provide access to the Workflow Monitor tool.

- To provide access to Workflow Monitor operations, in the **Workflow Monitor access** section, select the appropriate options as described in the following table:

Workflow Monitor access	
Option	Description
Use Workflow Monitor	Displays processes.
Distribute from Monitor	Distributes jobs to the nodes to which the user has access.
Delete from Monitor	Deletes parcels and documents.

Note: Selecting an option in the **Workflow Monitor access** area is the first step in providing access to Workflow Monitor. For more information on workflows, see [Chapter 5: Designing a Workflow](#).

10. To set user rights for annotations, in the **Annotation Security access** section, select the appropriate option as described in the following table:

Annotation Security access	
Option	Description
Create public annotations	Creates public annotations, which can be viewed and modified by all users.
Create private annotations	Creates private annotations, which can be viewed and modified only by the annotation's author.
Auditor	Views and maintains all annotations.

If **Auditor** is selected, the other options are selected automatically.

11. To set user privileges for viewing, activating, and deleting document versions, in the **Document Version control** section, select the appropriate options:

Document Version control	
Option	Description
View versions	Displays document versions.
Activate versions	Activates a previous document version to make it current.
Delete versions	Deletes a previous document version.

12. Click **OK**.
13. To close the **Add Level** window, click **Cancel**.

The new security level appears in the **Security Level Setup** window.

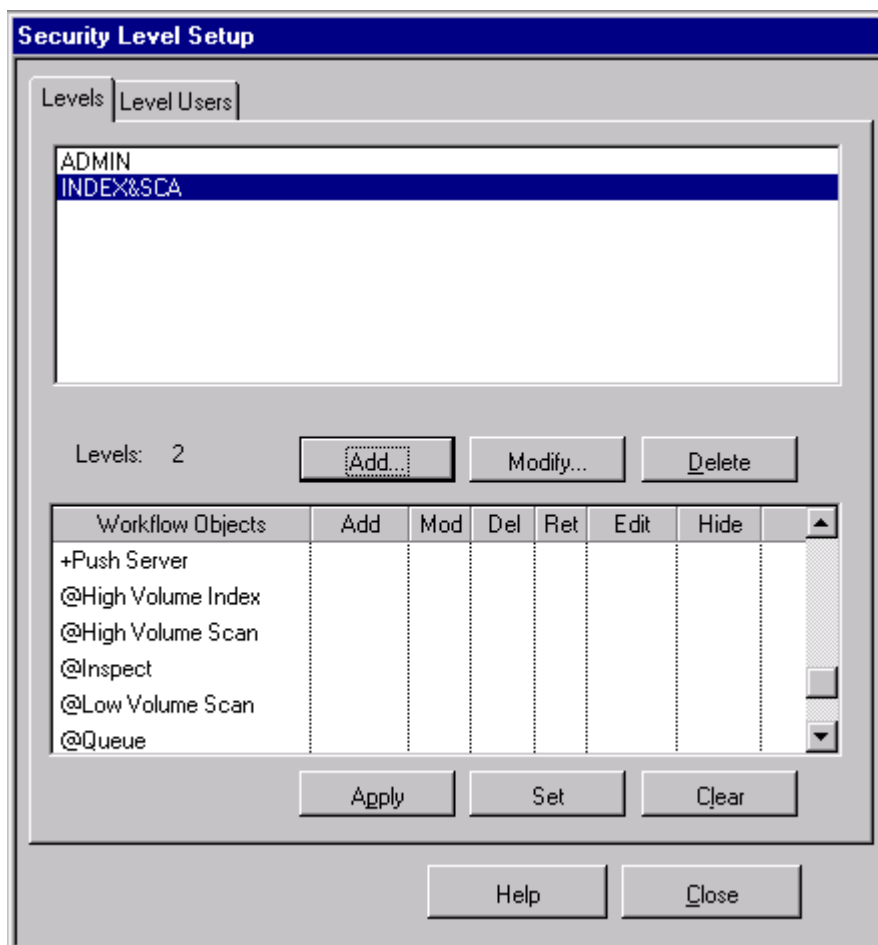


Figure 56: Managing the new security level

14. Select the new level in the list.

The access to workflow objects for the selected level is displayed in the **Workflow Objects** table.

An **X** indicates that this security level can perform the operation within the workflow object. When a new level is added, all cells are empty.

15. To select all operations, click **Set**.
16. To change the setting, click the corresponding cell.

The following table lists the operations in the **Workflow Objects** table:

Workflow Objects operations	
Operation	Description
Add	Adds new documents.
Mod	Modifies document records.
Del	Deletes existing documents.
Ret	Retrieves existing documents.

Workflow Objects operations	
Operation	Description
Edit	Edits imaged documents.
Hide	<p>Allows viewing, creating, and modifying hidden annotations.</p> <p>When working with ERM documents with secured form overlays, if the Hide option is not selected, fields with enabled field security are not shown in the ERM document. In this case, the users are also not able to edit these documents and view annotations created by other users.</p> <p>ERM documents that do not use presentation form overlays are not affected by this option.</p>

17. To clear all operations for all workflow objects, click **Clear**.

18. To modify a level, select it and click **Modify**.

For information on the **Modify Level** dialog, see [Modify Level Dialog](#).

19. To remove an unnecessary level, select it and click **Delete**.

20. To save changes made in the **Security Level Setup** dialog, click **Apply**.

Specifying the Security Settings for a Security Level

To specify the ACL based security settings for a security level, proceed as follows:

1. In the **Add Level** or **Modify Level** window, select the **ACL Security** tab.

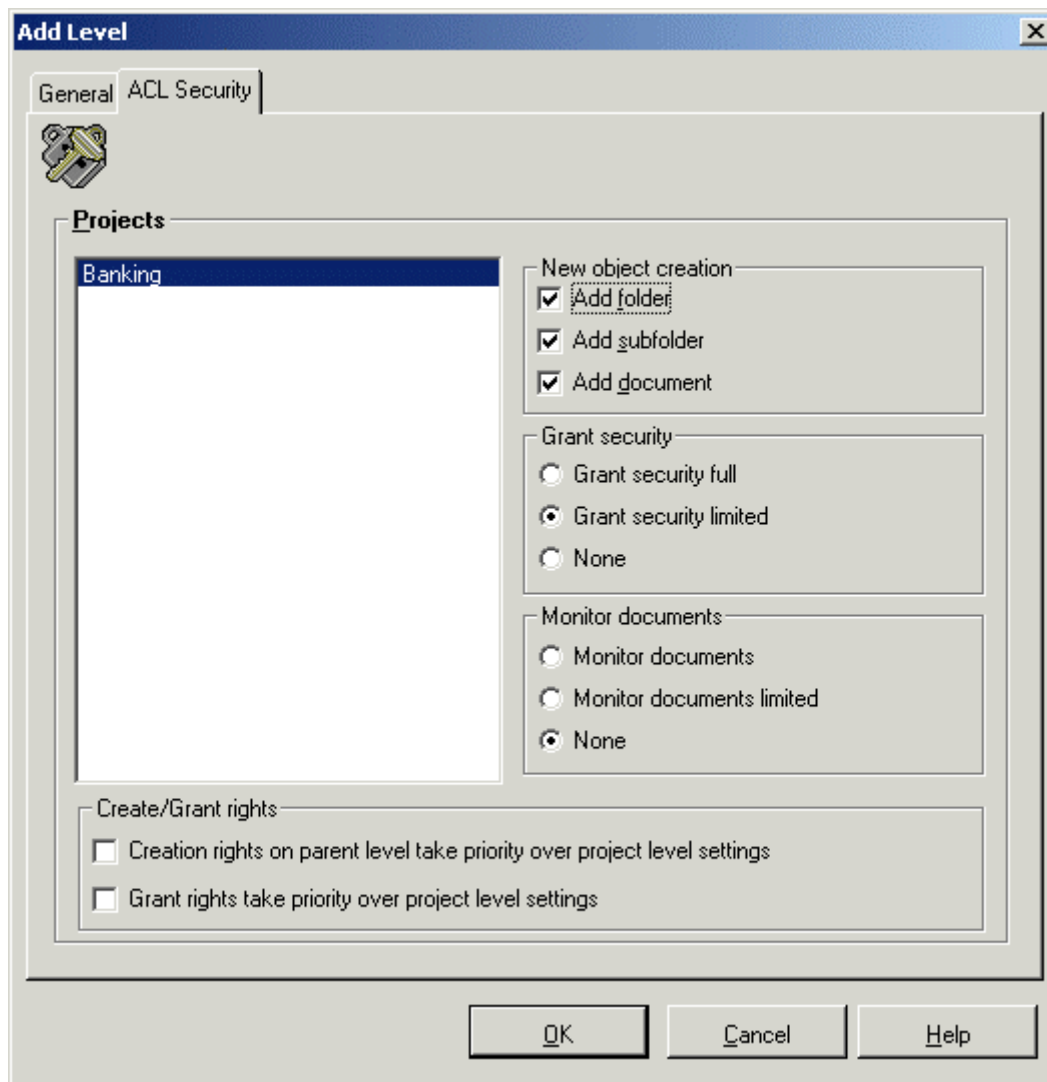


Figure 57: ACL Security tab

2. In the **Projects** list, select a project.
3. To specify that ACL based security settings determine the rights of users to create subfolders and documents, select **Creation rights on parent level take priority over project level settings**.

If this option is selected, users can create a subfolder only if the appropriate rights are assigned to that user or group for the parent folder. Users can create a document only if the appropriate rights are assigned to that user or group for the appropriate subfolder or folder.

4. To specify that the right to grant ACL based security to a document, folder, or subfolder is determined by ACL based security settings defined for that document, folder, or subfolder, select **Grant rights take priority over project level settings**.

If this option is selected, ACL based security settings for grant rights take priority over project level settings.

5. To set security level permissions, select the required options.

The following options are available:

Security level permission options	
Option	Description
Add folder	Users assigned to the selected security level can add a folder.
Add subfolder	Users assigned to the selected security level can add a subfolder.
Add document	Users assigned to the selected security level can add a document.
Grant security full	Users assigned to the selected security level can grant ACL based security rights for all documents, folders, and subfolders in the project.
Grant security limited	Users assigned to the selected security level can grant ACL based security rights only for those documents, folders, and subfolders to which the user has access. Only privileges possessed by the user can be assigned to documents.
None	Users assigned to the selected security level have no rights to grant ACL based security rights.
Monitor documents	Users assigned to the selected security level can view all documents, folders, and subfolders in Workflow Monitor. If this option is not selected, the user does not have access to Workflow Monitor for this project.
Monitor documents limited	Users assigned to the selected security level can view only the documents, folders, and subfolders in Workflow Monitor to which they have read access.
None	Users assigned to the selected security level cannot open Workflow Monitor.

6. To save changes and close the window, click **OK**.

Security Level Setup Dialog

Security levels are set up for the following reasons:

- to provide access to specific applications within Exigen Workflow
- to assign access to workflow objects and the level of access within the objects

Each user must be assigned a security level during setup.

The upper half of the **Security Level Setup** dialog lists all existing security levels for the Exigen Workflow system. Buttons common to both tabs are described in the following table:

Security Level Setup buttons	
Button	Description
Add	Opens the Add Level dialog box to add a new security level.
Modify	Opens the Modify Level dialog box to change the attributes of the selected security level.
Delete	Deletes the selected security level.
Close	Closes the current window and saves any changes made.
Help	Displays Help.

The **Security Levels** dialog has the following two tabs:

- [Levels Tab](#)
- [Level Users Tab](#)

Levels Tab

The **Levels** tab is used to assign operations that the users with this selected security level are allowed to perform.

An **X** in a table cell indicates that the security level selected in the top table can perform that operation within the corresponding workflow object. Columns in the **Workflow Objects** table of the **Levels** tab represent the following operations:

Workflow Objects table	
Column	Operation
Add	Adds new documents.
Mod	Modifies document records.
Del	Deletes existing documents.
Ret	Retrieves existing documents.
Edit	Edits document images.
Hide	Allows viewing, creating, and modifying hidden annotations. When working with ERM documents with secured form overlays, if the Hide option is not selected, fields with enabled field security are not shown in the ERM document. In this case, the users are also not able to edit these documents and view annotations created by other users. ERM documents that do not use presentation form overlays are not affected by this option.

A new project is assigned all previously defined levels. If no levels are defined, only the ADMIN level is shown. The ADMIN level allows user access to all workflow objects. The **Workflow Objects** table shows the registered workflow objects and the operations available for the selected security level.

The following buttons are available in the **Workflow Objects** table:

Workflow Objects table	
Button	Description
Apply	Saves changes made in the Security Level Setup window.
Set	Selects all operations for all workflow objects.
Clear	Clears all operations for all workflow objects.

Level Users Tab

The **Level Users** tab is used to view all users assigned to a selected security level.

Note that users cannot be added or removed from this list in the **Level Users** tab. This is done separately by assigning a user an appropriate security level when adding a user to the system. For information on adding a user, see [Adding a New User](#).

Add Level Dialog

The **Add Level** dialog is used to add a security level.

The following table describes the **Add Level** dialog:

Add Level dialog	
Element	Description
Security level	Security level name.
Synchronization info	Information used for NT and Exigen Workflow user synchronization. It includes the name of a Windows NT workgroup or the path to the directory.
Database role	<p>User database roles are as follows:</p> <p>User allows reading table data.</p> <p>Administrator allows creating tables and maintaining table fields.</p> <p>This field is available only for Oracle and SQL databases.</p>
System access	Options that provide users assigned to this level access to specific Exigen Workflow features.
Administrator	<p>Administrator utilities such as the following:</p> <ul style="list-style-type: none"> • system setup • project configuration • optical functions <p>This option also grants access to Audit Viewer, Users Synchronization Setup, and the SQL Talk utility, which allows users to modify the Exigen Workflow database by writing SQL statements.</p> <p>SQL Talk is not available if it is disabled in the <code>visiclt.ini</code> file located in the Windows directory.</p> <p>In <code>visiclt.ini</code> file, the status of SQL Talk is defined by the <code>sql_talk</code> parameter in the <code>[setup_system_access]</code> section as follows:</p> <ul style="list-style-type: none"> • If the Administrator option is selected and the value of the <code>sql_talk</code> parameter is set to 1, SQL Talk is available to users with the defined security level. • If the value of the <code>sql_talk</code> parameter is set to 0, SQL Talk is not available to users even if the Administrator option is selected in the security level setup.
Project Builder/Setup	Project Builder application and Configuration function.
Statistics	Statistics application.
Table Maintenance	Administrator utility and table maintenance function.
Utilities	<p>Workflow Viewer, Exigen Workflow database, and image utilities listed in Utilities folder in Administration Tools in Exigen Workflow Explorer.</p> <p>When the Utilities check box is selected, the Process Monitor icon is displayed in Exigen Workflow Explorer but Process Monitor cannot be started.</p>
Workflow Builder	Workflow Builder, Workflow Viewer, Component Configuration Manager, and E-Capture Administrator.
Print Server/Monitor	Print Server and Print Monitor applications.
Process Monitor	Process Monitor application.
Configuration Browser	Configuration Browser application.

Add Level dialog	
Element	Description
Workflow Monitor access	Options that provide access to the Workflow Monitor and Process Monitor tools.
Use Workflow Monitor	Views processes in Workflow Monitor and Process Monitor.
Distribute from Monitor	Distributes jobs to the nodes to which the user has access.
Delete from Monitor	Deletes parcels and documents.
Annotation Security access	Options that provide users access to annotations.
Create public annotations	Creates public annotations.
Create private annotations	Creates private annotations.
Auditor	Views and maintains all annotations.
Document Version control	Options that allow viewing, activating, and deleting document versions.
View versions	Views document versions.
Activate versions	Activates a previous document version to make it current.
Delete versions	Deletes a previous document version.
OK	Creates the new security level.
Cancel	Closes the current window.
Help	Displays Help.

Additional Workflow Monitor security options are assigned in the Workflow Designer application as described in [Setting Up Workflow Objects](#).

Modify Level Dialog

The **Modify Level** dialog is used to modify the name of a security level and other security level information.

This dialog has the same fields as the **Add Level** dialog as described in [Add Level Dialog](#).

Specifying Access Levels

Access levels restrict access to specific folders and subfolders. Access level setup consists of defining the access level name and assigning users to the access levels. Access levels are set up and maintained in the **Folder/Subfolder Security Group Setup** window.

When setting up access levels, determine which types of folders and subfolders must be restricted. You can set up multiple levels to restrict multiple types. Keep a record of which levels apply to which types, as this information must be provided to the indexers to ensure that the correct access levels are assigned during indexing.

To set up access levels, proceed as follows:

1. Click **Folder/Subfolder Security Groups**.



The **Folder/Subfolder Security Group Setup** window appears.

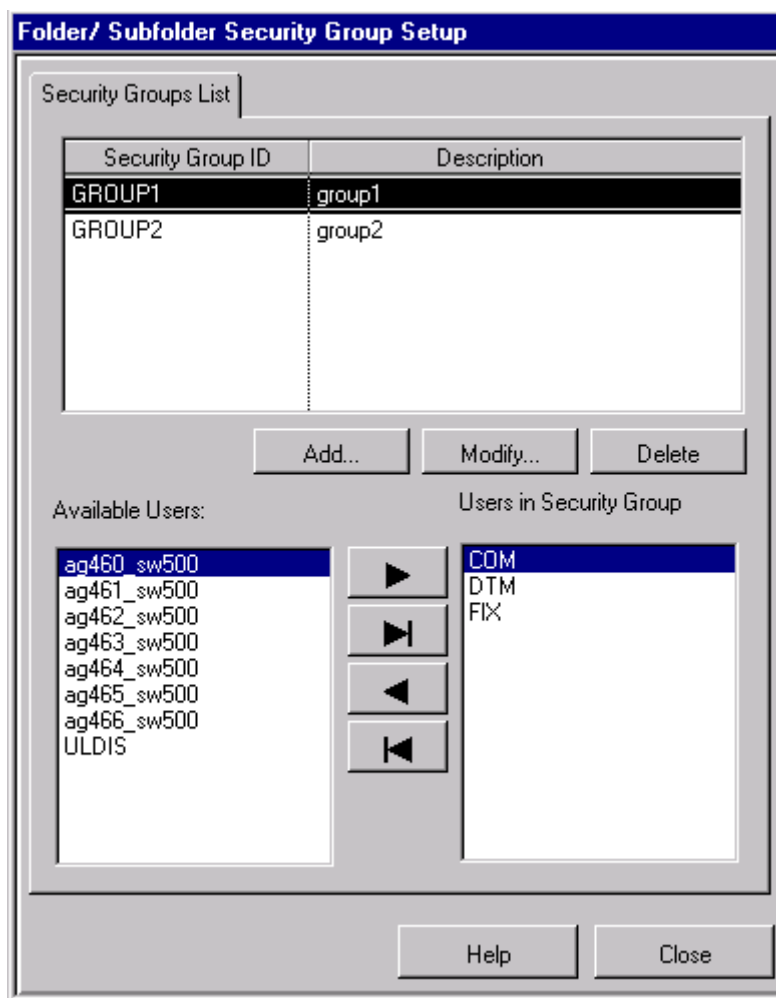


Figure 58: Folder/Subfolder Security Group Setup window

2. To add an access level group, click **Add**.

The **Add Folder/Subfolder Security Level** window appears.



Figure 59: Adding a new access level

3. In the **Security Group ID** field, enter the security group ID.
4. In the **Description** field, enter the security group description.
5. Click **OK**.
6. To close this window, click **Cancel**.

The access level is displayed in the top table of the **Folder/Subfolder Security Group Setup** window.

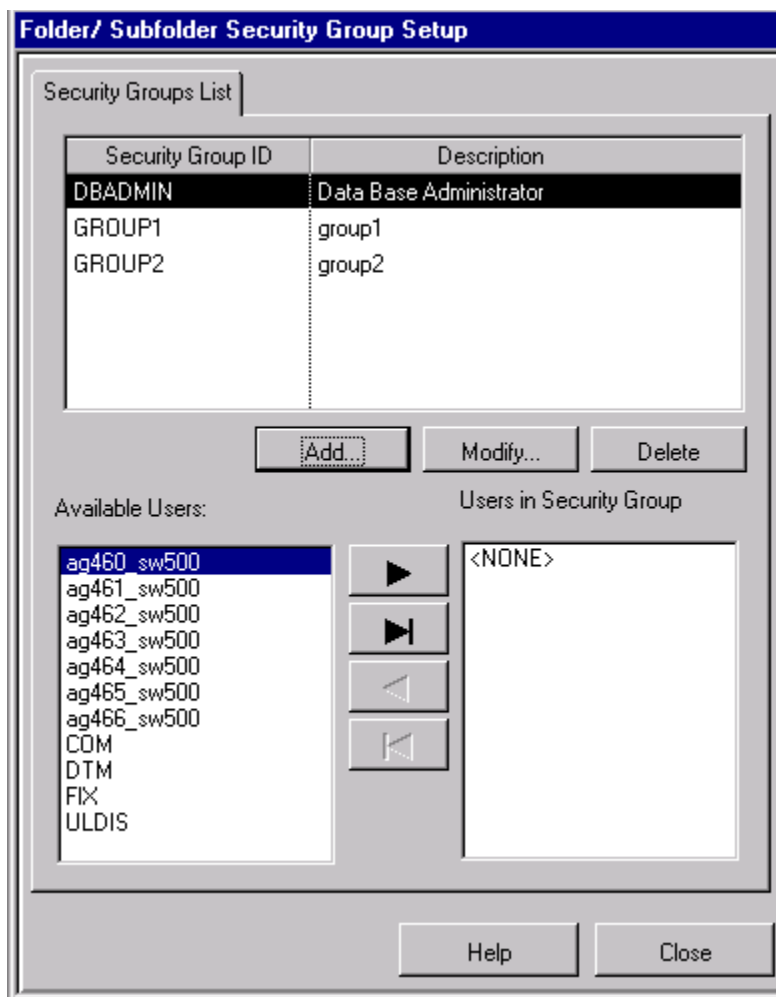






Figure 60: Adding users to an access level

The table at the top of the window displays the list of access level groups. At the lower left is the list of users in the system. At the lower right is a list of users assigned to the selected group.

7. To add a user, select the user name in the left list, and click **Add User** .
8. To add all users to the access level, click **Add All Users** .
9. To remove a user, select the user name in the list on the right, and click **Remove User** .
10. To remove all users from the access level, click **Remove All Users** .
11. To modify an access level, select the level and click **Modify**.
12. To remove an access level, select the level and click **Delete**.

Setting Up Workflow Objects

Workflow Objects are process tools on a workflow map such as scanning, indexing and retrieval. The standard workflow objects are as follows:

- High Volume Scan
- Low Volume Scan
- Barcode Server
- High Volume Index
- Inspect
- Queues
- Retrieve
- Work Item Submitter
- Commit

Setting up workflow objects also includes defining which security levels can access each workflow object and which operations can be performed from each object by users of these security levels.

Although Exigen Workflow contains all the workflow objects previously listed, you may need to add a new one in the future. A workflow object cannot be added to a workflow map until it is set up in the system.

To set up a workflow object, proceed as follows:

1. Click **Workflow Objects Setup**.



The **Workflow Object Setup** window appears.

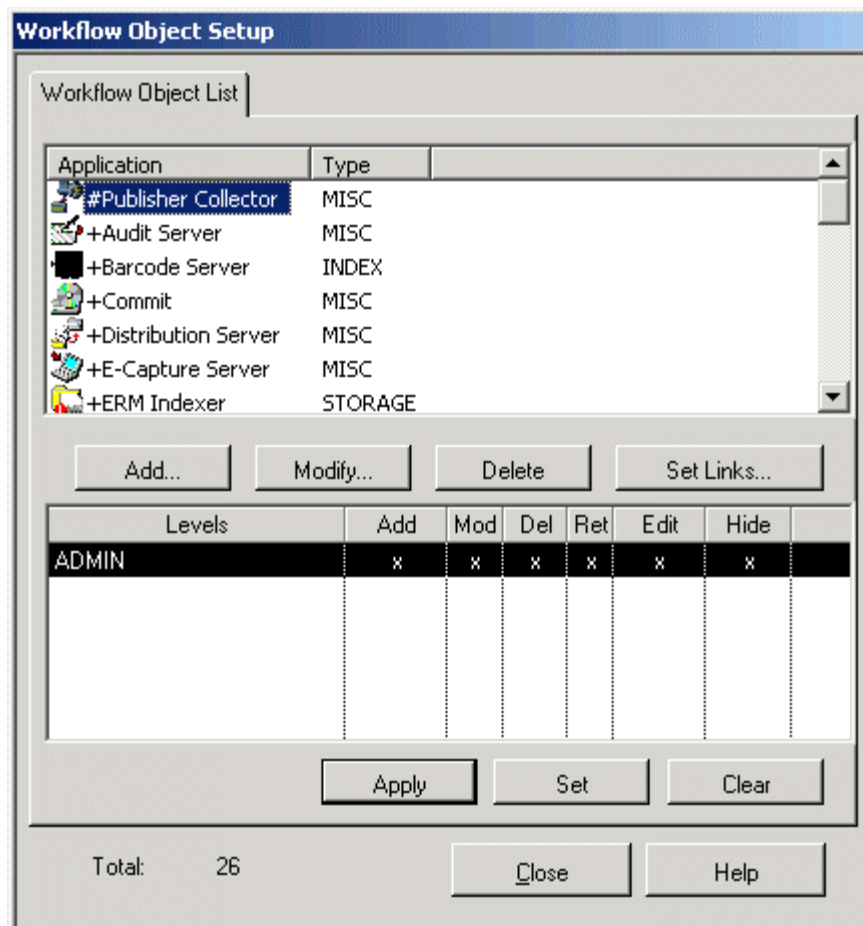


Figure 61: Workflow Object Setup window

The table at the top lists all workflow objects registered in the system. The security levels in the system and the application operations each level can perform in the selected workflow object are listed in the lower section. Security level access can be assigned using the same procedures as described in [Specifying Security Levels](#).

2. To add a new workflow object, click **Add**.

The **Add Workflow Object** window appears.

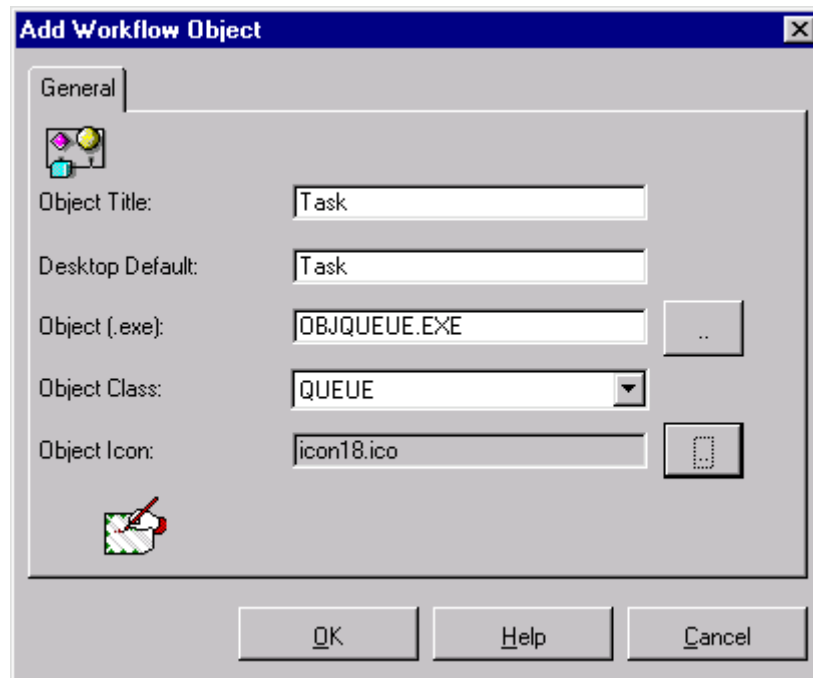


Figure 62: Adding a new workflow object

3. In the **Object Title** field, enter the name of the object.

This is the value displayed in the **Workflow Objects Setup** window.

4. In the **Desktop Default** field, enter the default name to appear when the object is added to the workflow.
5. To locate the workflow object executable, click the browse button next to the **Object (.Exe)** field. Select an **Object Class** from the corresponding list box, depending on the executable selected.
6. To change the default icon for the object, click the browse button next to the **Object Icon** field and select a new icon.
7. When all values are set, to add the object, click **OK**.

The new object appears in the main object list.

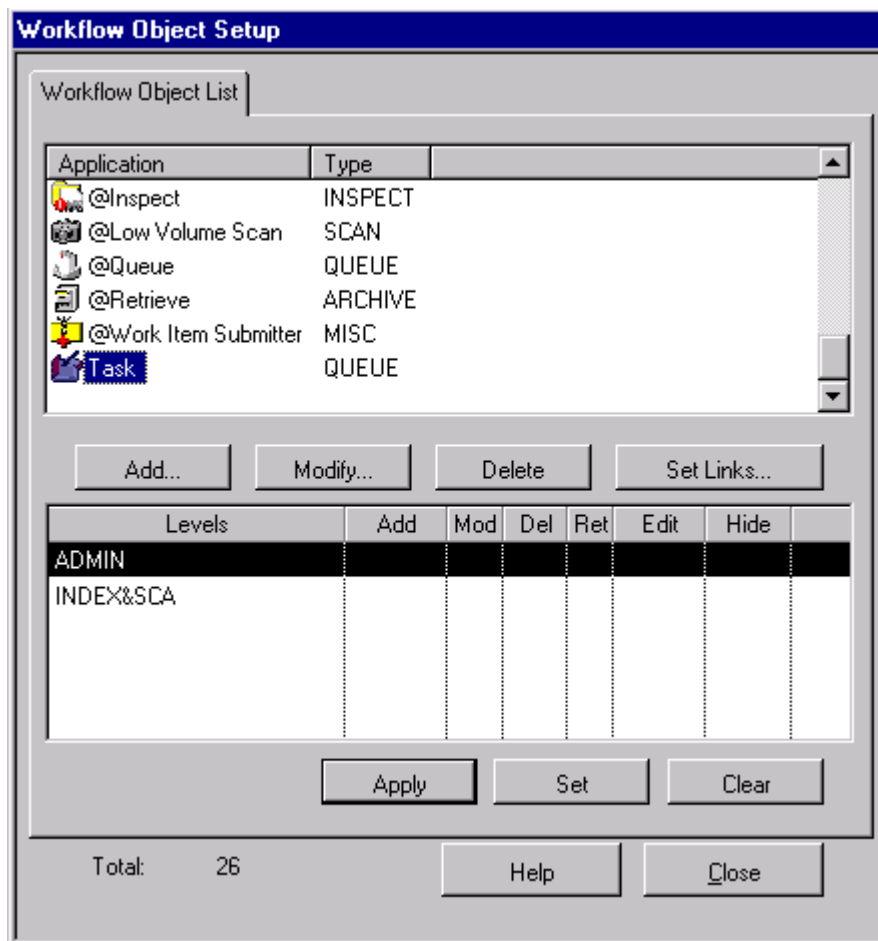


Figure 63: New workflow object

8. To change settings, select the desired object and click **Modify**.
9. To remove the object, select the desired object and click **Delete**.

Relationships between workflow objects are the links that can be established between workflow objects on a workflow map. For each workflow object, you must define where the documents or batches are allowed to travel sequentially through the workflow.

If batches or documents must move back and forth between two workflow objects, the two workflow objects must be allowed to link to one another.

For example, if you want indexed documents to be sent to the Inspect queue and then sent back to the Index queue, you must define Inspect as an allowed link to Index and Index as an allowed link to Inspect.

10. To view or modify the links for a specific workflow object, select the object and click **Set links**.

The **Set Links** dialog appears.

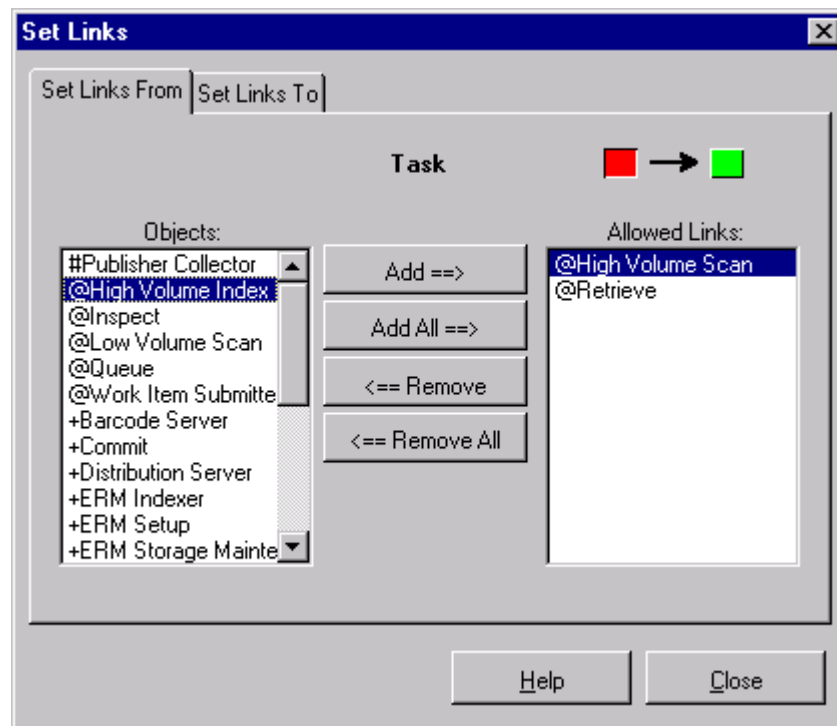


Figure 64: Setting links from a workflow object

In the **Set Links From** tab, the **Object** box displays all workflow objects.

11. To make an object an **Allowed Link** destination object, select it and click **Add**.

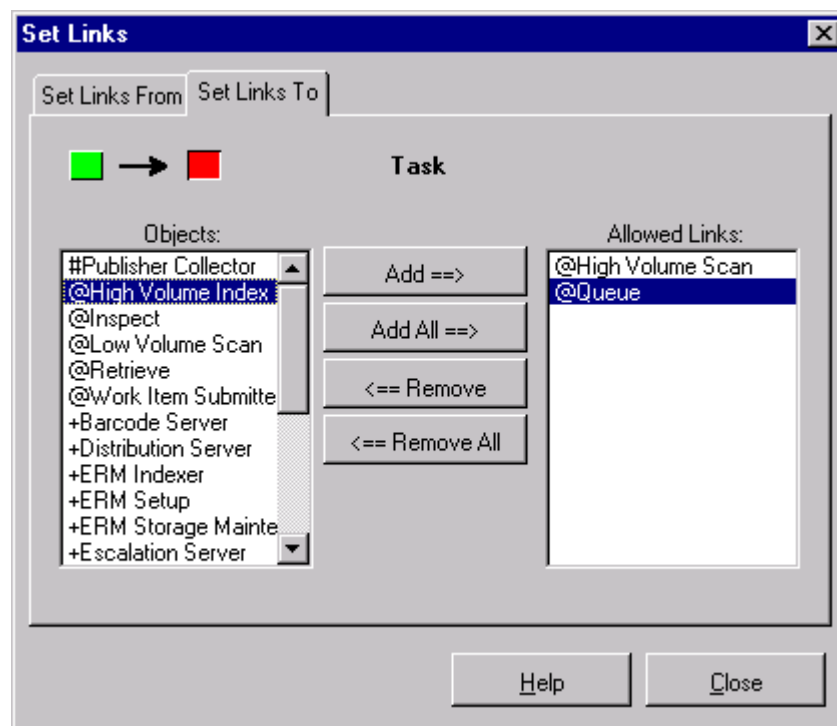


Figure 65: Setting links to a workflow object

In the **Set Links To** tab, the **Object** box displays all workflow objects.

12. To make an object an **Allowed Link** source object, select it and click **Add**.
13. To move objects to or from the **Allowed Links** lists, click the arrow buttons in both tabs.

The **Workflow Object Setup** window can also be used to create special workflow objects, named task definitions, which are used for Task Oriented Workflow (TOW). For information on creating task definitions, see the *Task Oriented Workflow Administrator's Guide*, Chapter 2: Creating Task Definitions.

Setting Up Workflow Groups

A **Workflow Group** groups users by department or by work function. Users can belong to more than one workflow group, and a workflow group can have users with different security levels.

To organize users into groups, proceed as follows:

1. Click **Workflow Group Setup**.



The **Workflow Group Setup** window appears.

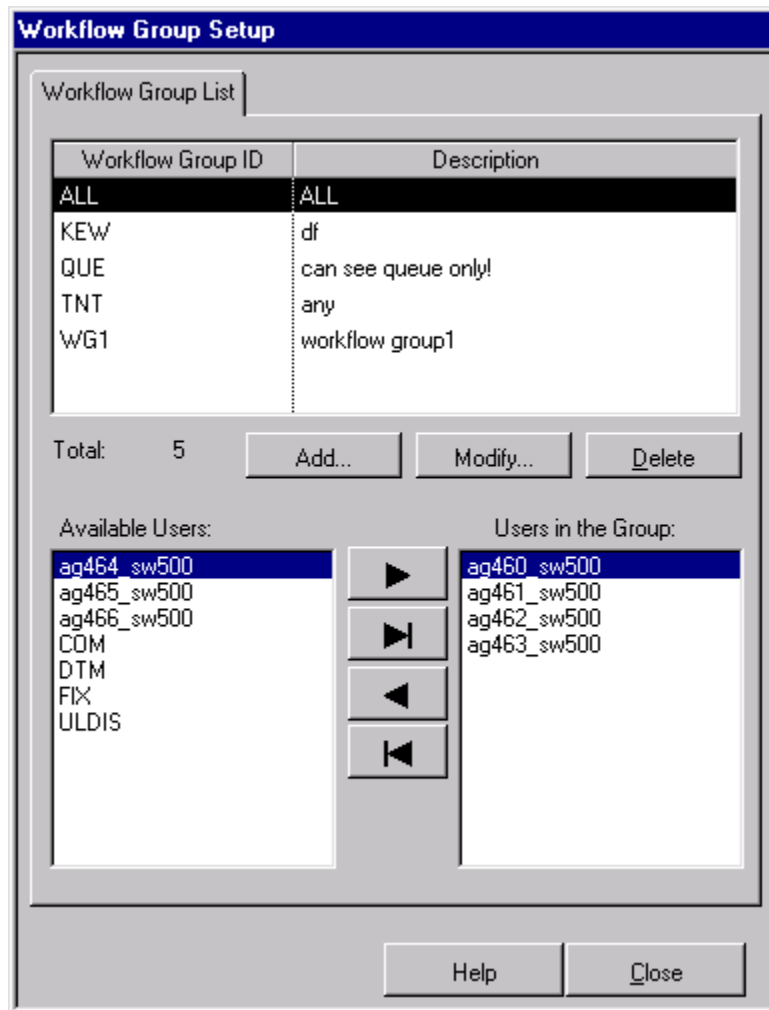


Figure 66: Workflow Group Setup window

The table at the top lists all defined workflow groups. The **Available Users** list shows all available users in the system.

2. To add a workflow group, click **Add**.

The **Add Group** window appears.

Figure 67: Adding a new group

3. In the **Add Group** window, enter the **Workflow Group ID**, which must have a maximum of three characters, and its description.
4. To use NT and Exigen Workflow user synchronization, proceed as follows:
 - In the **Synchronization Info** field, enter the name of a Windows NT workgroup or the path to the directory.
 - Select the authentication mode defaults for synchronized users.

You can select one or several modes. For Win 32® and CCID Win32 authentication modes, you can specify a database user type.

Note: The **Database Authentication** option and the **Database User type** list box are available only if extended security is used.

- To synchronize users in the new workflow group with a global group, in the **Global Group** list box, select a global group.

When ADSync synchronizes the new workflow group with an external workgroup, users in this workflow group are also synchronized with the global group selected in the **Global Group** list box.

For information on authentication mode defaults, see [Specifying the Authentication Mode](#).

For information on user synchronization, see [Chapter 10: Setting Up User Synchronization Service](#).

5. To accept the settings, click **OK**.
6. To close the window, click **Cancel**.

The new group is listed in the **Workflow Groups Setup** window.

7. To add a user to the group, select the user name in the **Available Users** list and click **Add User**



8. To add all users to the group, click **Add All Users**



9. To remove a user, in the **Users in Group** list, select the user name and click **Remove User**



10. To remove all users from the group, click **Remove All Users**



Note: Adding a common user such as the default COM and FIX to a group has special meaning and adds special behavior to your workflow. For more information on users, see [Regular and Common Users](#).

11. To modify a group, select it in the **Workflow Group List** and click **Modify**.
12. To remove a group, click **Delete**.

Setting Up Corporate Locations

Corporate Locations are used to identify geographical locations or branch offices where users are located. If your company has many people performing the same functions in different cities or states, corporate locations allows you to restrict where users can send parcels. Users can have the option to see all users, regardless of location, if required.

To set up corporate locations, proceed as follows:

1. Click **Corporate Locations Setup**.



The **Locations Setup** window appears with the **Corp. Location List** tab opened.

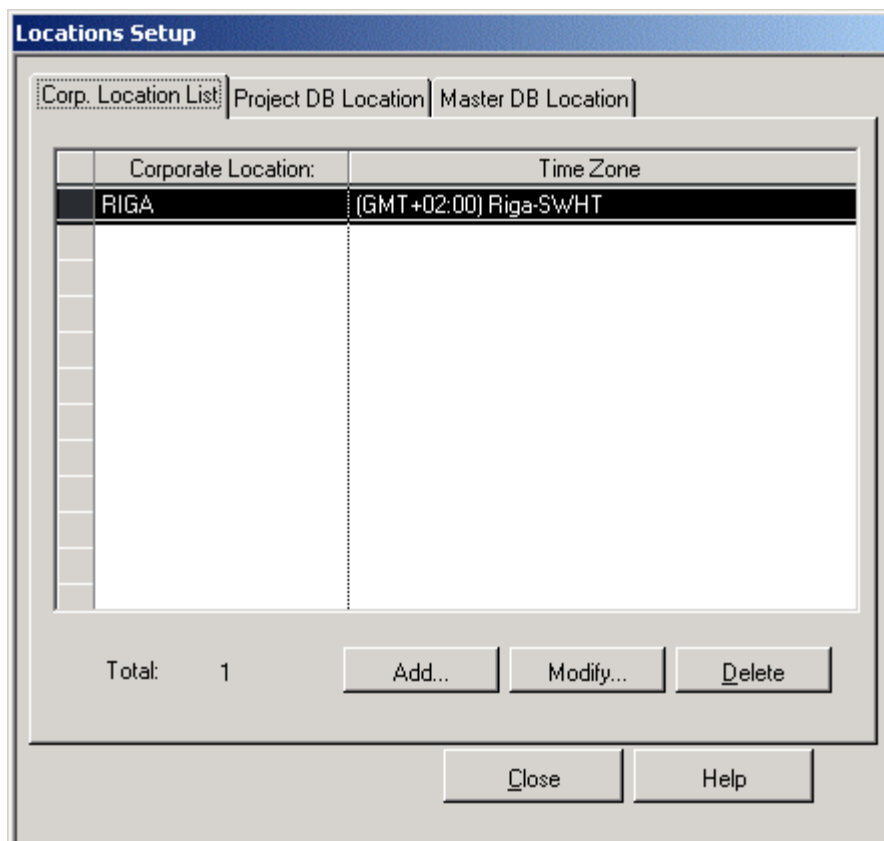


Figure 68: Locations Setup window

The **Corp. Location List** tab displays the general corporate location properties such as location name and time zone. Time zone definition is used to resolve date and time discrepancies between database servers and local computers.

For each location, the time difference relative to Greenwich Mean Time (GMT) is shown in the brackets in the **Time Zone** column.

2. In the **Locations Setup** window, assign time zones for corporate locations, projects, and system tables.

User time zones are specified by assigning a corporate location in the **User Setup** window as described in [Adding a New User](#).

Exigen Workflow system tables store the time and date by project database location, but the local time is displayed for the user.

The **Project DB Location** tab shows a time zone assigned for your project.

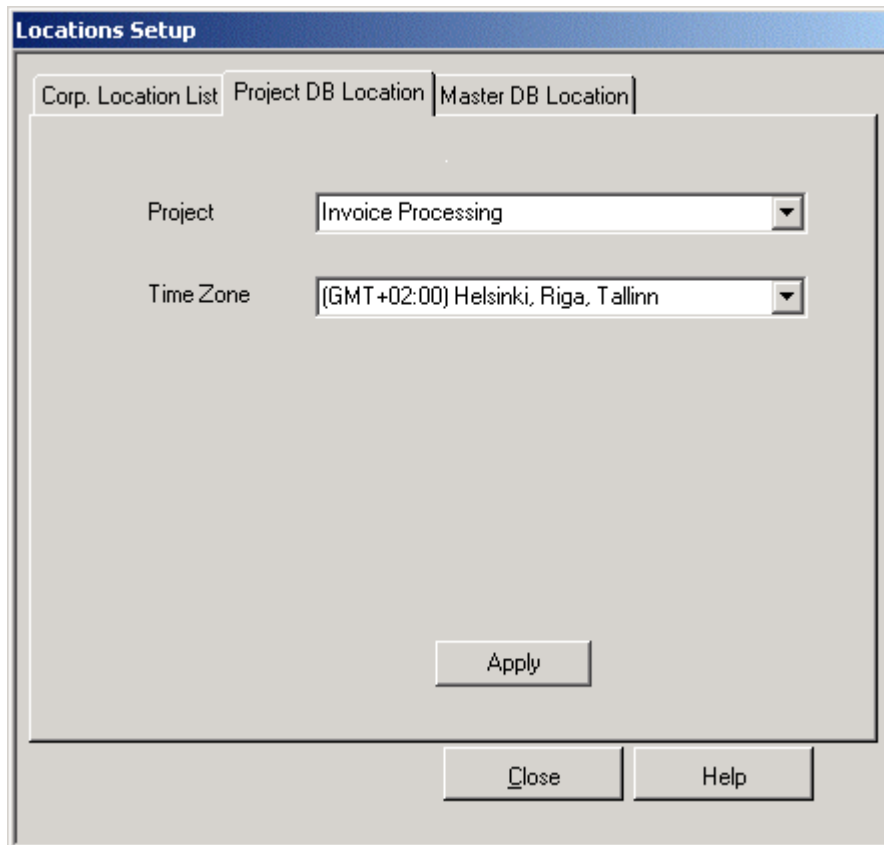


Figure 69: Project DB Location tab in the Locations Setup window

To assign a time zone for your project, proceed as follows:

1. In the **Project DB Location** tab, select the project.
2. Select the corresponding time zone.
3. Click **Apply**.

Do not change the time zone for an active project, as the change can cause unexpected results.

The **Master DB Location** tab displays a time zone assigned for the Exigen Workflow system tables or Master DB. If the system tables are stored on the same server or in the same database as the project, the Master DB location time zone must match the Project DB location time zone.

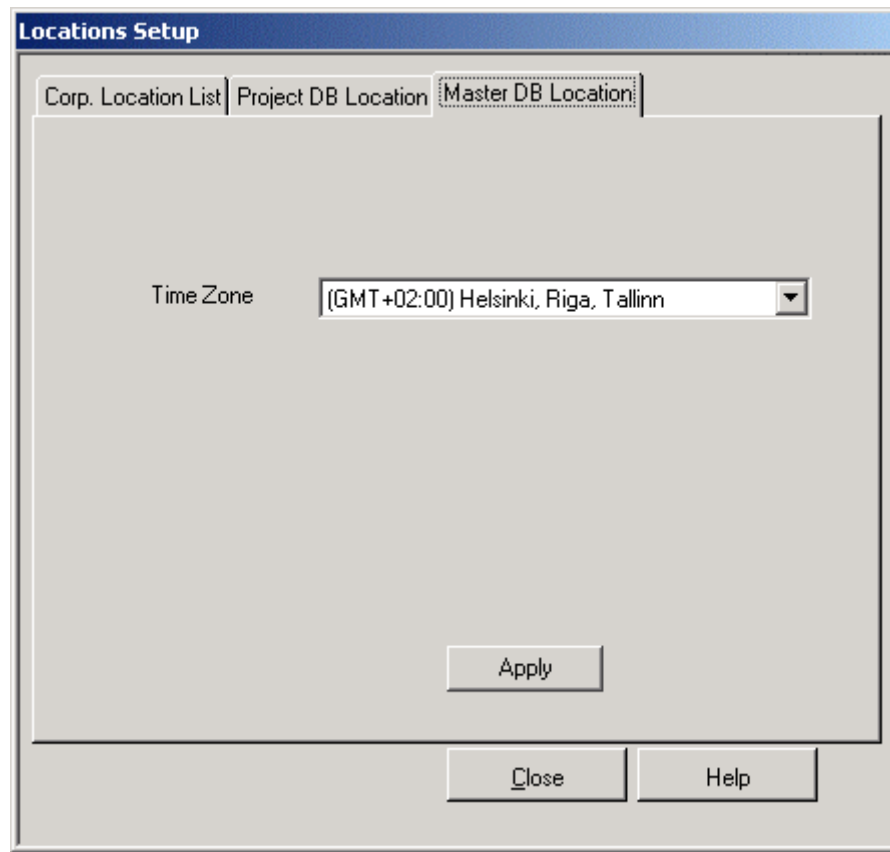


Figure 70: Master DB Location tab in the Locations Setup window

Note: After any date or time change on the database server or master database and project database server, if they are separate, the time zone settings must be changed manually to reflect changes. Daylight savings time is not supported in Exigen Workflow. If a location requires daylight savings time, the location must be changed to actually match the time offset from GMT.

In the **Locations Setup** window, you can perform the following tasks:

- [Adding a Corporate Location](#)
- [Modifying a Corporate Location](#)
- [Deleting a Corporate Location](#)

Adding a Corporate Location

To add a corporate location, proceed as follows:

1. Click **Add**.

The **Add Corp. Location** window appears.

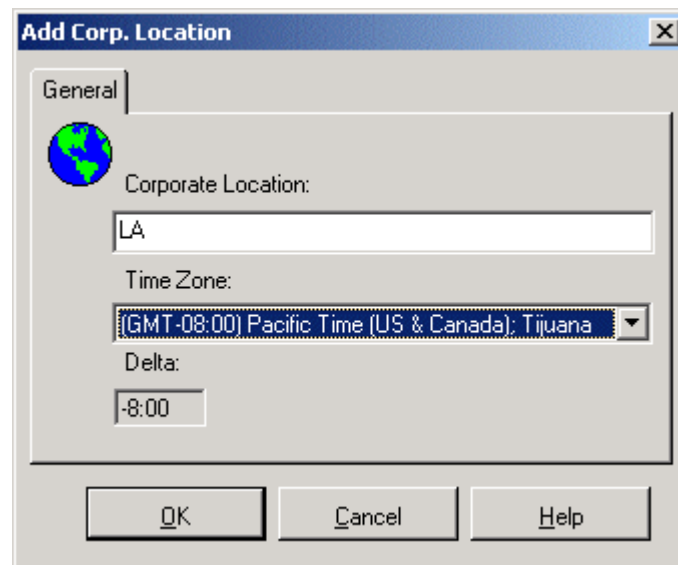


Figure 71: Add Corp. Location window

2. In the **Corporate Location** field, enter the location name.
3. Select the corresponding time zone and click **OK**.

The **Delta** field shows the time difference relative to GMT.

4. To close this window, click **Cancel**.

The newly created corporate location appears in the **Locations Setup** window.

5. To assign the time zone for the project, select the **Project DB Location** tab.
6. Select the project and the corresponding time zone.
7. Click **Apply**.
8. To assign the time zone for system tables, click **Master DB Location**.
9. Select the time zone and click **Apply**.

Modifying a Corporate Location

To modify a corporate location, proceed as follows:

1. Select the location and click **Modify**.

The **Modify Corp. Location** window appears.

This window is similar to the **Add Corp. Location** window.

2. Change the location name and time zone.
3. To save the changes, click **OK**.

Deleting a Corporate Location

To delete a corporate location, proceed as follows:

1. Select the location and click **Delete**.

The confirmation window appears.

2. To delete the location, click **Yes**.

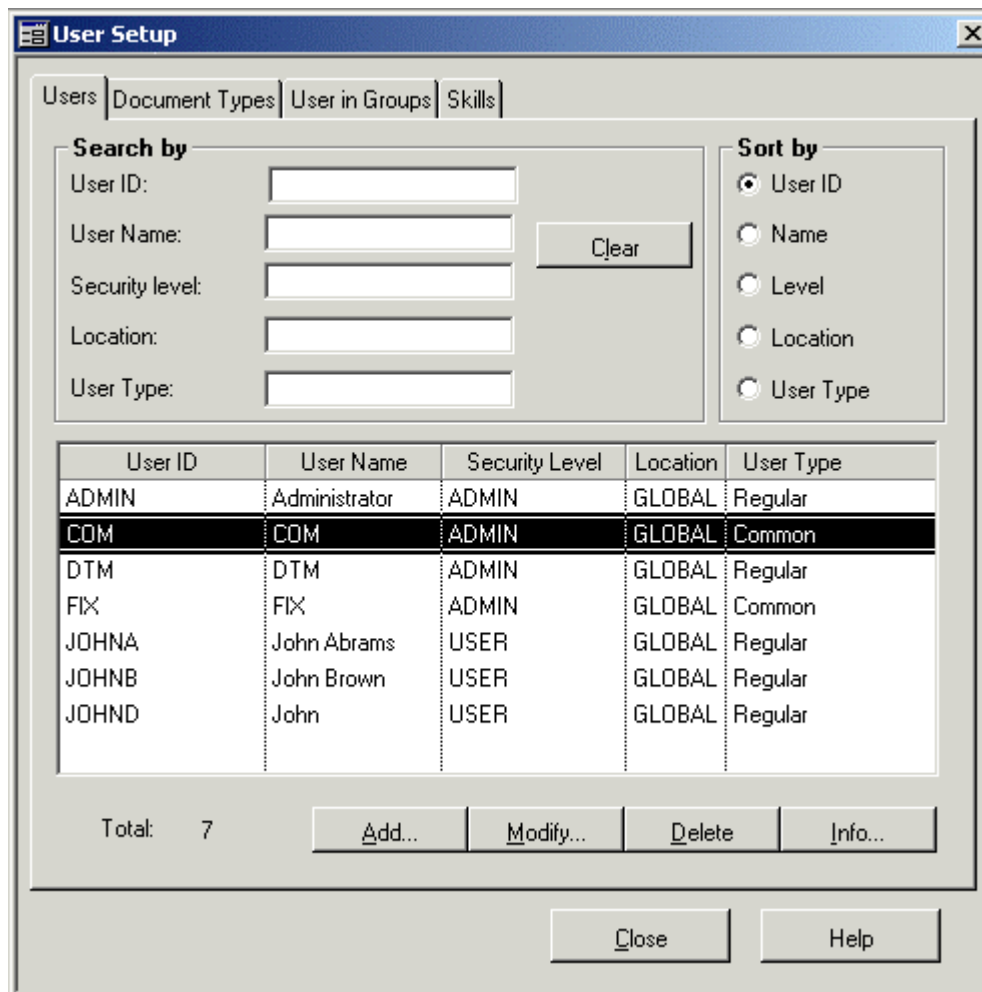
Setting Up Users

User Setup maintains user access rights. User setup includes issuing each user a unique ID and an initial password, and defining permissions for security levels and document types. Users must be set up before they can log onto Exigen Workflow and access any application or document.

To manage users, proceed as follows:

1. Click **Workflow Users Setup** .

The **Users Setup** window appears.



The **User Setup** window is shown with the **Users** tab selected. It features search and sort filters, a table of users, and action buttons.

Search by:

User ID:
 User Name:
 Security level:
 Location:
 User Type:

Sort by:

☒ User ID
☐ Name
☐ Level
☐ Location
☐ User Type

User ID	User Name	Security Level	Location	User Type
ADMIN	Administrator	ADMIN	GLOBAL	Regular
COM	COM	ADMIN	GLOBAL	Common
DTM	DTM	ADMIN	GLOBAL	Regular
FIX	FIX	ADMIN	GLOBAL	Common
JOHNA	John Abrams	USER	GLOBAL	Regular
JOHNB	John Brown	USER	GLOBAL	Regular
JOHND	John	USER	GLOBAL	Regular

Total: 7

Figure 72: User Setup window

The **Search by** and **Sort by** sections display the search and sort tools.

2. To narrow the list of users in the table, enter a value in any of the fields.
3. To sort the list in a specific order, select the appropriate radio button.

The default sort order is alphabetical by User ID.

The **Document Types** tab shows document types the user can access.

4. If required, configure these settings as described in [Specifying Document Types a User Can Access](#).

The **User in Groups** tab shows which groups a user belongs to. These settings are not described in this section.

5. To change the group settings, use the **Workflow Groups** tool.
6. To assign skills to users, select the **Skills** tab and follow instructions as described in [Assigning Skills to Users](#).

For information on the Workflow Groups tool, see [Setting Up Workflow Groups](#).

In the **User Setup** window, you can perform the following tasks:

- [Adding a New User](#)
- [Specifying the Authentication Mode](#)
- [Specifying Document Types a User Can Access](#)

Adding a New User

To add a new user, proceed as follows:

1. Click **Add**.

The **Add User** window appears.

The screenshot shows the 'Add User' dialog box with the 'General' tab selected. The fields are as follows:

Field	Value
Name	Timothy Smith
User ID	TIM
Login ID	TIM
Level	ADMIN
User Type	Regular (selected from dropdown)

Figure 73: Add User window, adding a new user's general info

The window consists of the following tabs:

- **General**
- **Address**
- **Corporate**
- **Advanced**
- **Synchronization**
- **Authentication**
- **Password**

2. In the **General** tab, enter general information about the user:

General tab	
Field	Description
Name	User name.
User ID	User ID, which is used to route parcels and documents. User ID cannot exceed 32 characters.
Login ID	Login ID. All users need a Login ID to log into Exigen Workflow.
Level	User's security level as described in Specifying Security Settings .
User Type	User type as described in Regular and Common Users .

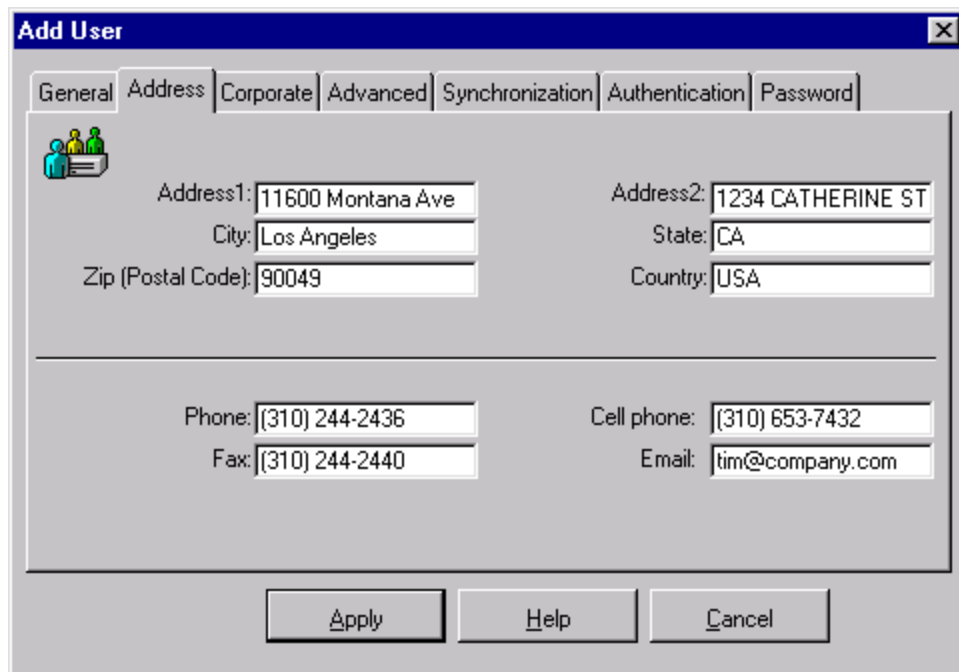
The image shows a Windows-style dialog box titled "Add User". It has a tabbed interface with tabs for "General", "Address", "Corporate", "Advanced", "Synchronization", "Authentication", and "Password". The "Address" tab is currently selected. On the left side of the tab, there is a small icon of three people. The main area of the dialog contains several text input fields. The "Address1" field contains "11600 Montana Ave", "City" contains "Los Angeles", and "Zip (Postal Code)" contains "90049". The "Address2" field contains "1234 CATHERINE ST", "State" contains "CA", and "Country" contains "USA". Below these, there are fields for "Phone" (containing "(310) 244-2436"), "Fax" (containing "(310) 244-2440"), "Cell phone" (containing "(310) 653-7432"), and "Email" (containing "tim@company.com"). At the bottom of the dialog, there are three buttons: "Apply", "Help", and "Cancel".

Figure 74: Add User window, adding a new user's address

3. In the **Address** tab, enter physical addresses and email addresses for the user.

The **Phone** field in the figure shows the default U.S. phone format mask, PhoneMask="(999) 99999". Local versions use the phone format mask specified in the [INT] section of the Visi.ini file.

Email addresses must be preceded by the following:

smtp:

The screenshot shows the 'Add User' dialog box with the 'Corporate' tab selected. The 'Corporate' tab contains the following fields:

- Corp. Location: GLOBAL
- Position: ASSISTANT
- Supervisor: DTM
- Manager: DTM
- Executive: DTM

Buttons at the bottom: Apply, Help, Cancel.

Figure 75: Add User window, adding a new user's corporate info

- In the **Corporate** tab, define a user's position within the company's corporate structure.

The following fields are available:

Corporate tab	
Field	Description
Corp Location	Branch office where a user is located. A list of existing locations is available. The default location is Global. For information on defining other locations, see Setting Up Corporate Locations .
Position	User's job title, for example, assistant, manager, or technician.
Supervisor, Manager, Executive	Chain of command within the company. A value is chosen from a list of all users in the system. These fields are used to notify the Supervisor if a parcel is in a user's queue for 7 days, the Manager after 14 days, and the Executive of the department after 21 days.

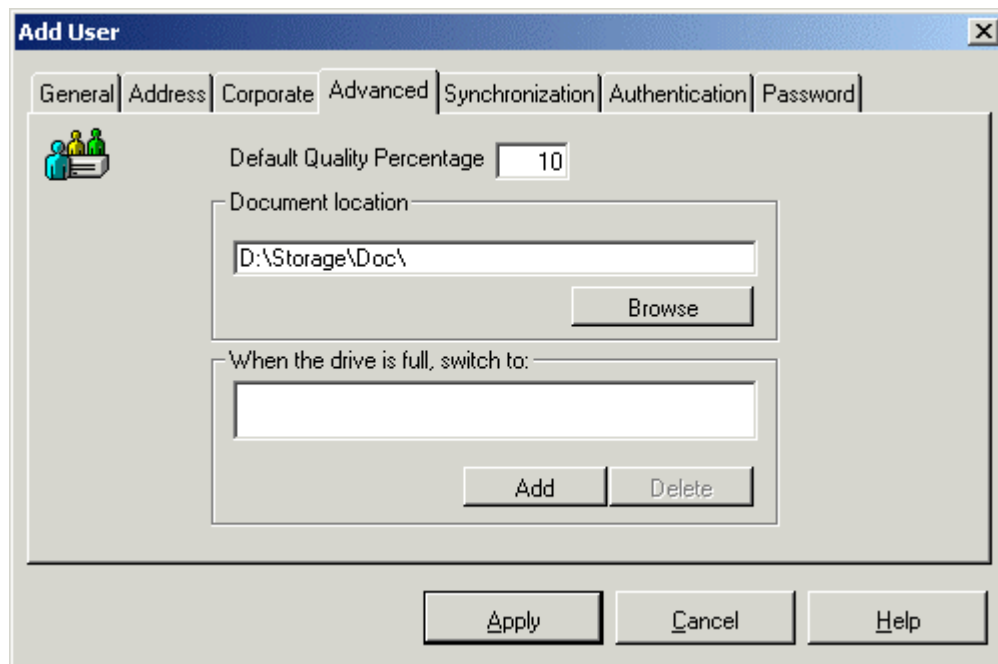


Figure 76: Add User window, adding a new user's document location

5. Select the **Advanced** tab.
6. In the **Default Quality Percentage** field, enter a numeric value from 0 to 100.

This value is used by Automatic Queue Server handlers to determine what percentage of parcels processed by the user are sent to the quality control node. The larger this value is, the more parcels are routed through the quality control cycle.

7. If required, assign a specific document location for a user. If the user scans documents and you want to override the scan location set up in the configuration process, enter a file path.
8. To specify whether the user is synchronized with directory services, in the **Synchronization** tab, select an option.

User synchronization significantly reduces the administrative tasks required to maintain two separate sets of security settings: in Windows NT and in Exigen Workflow. For more information on synchronizing security settings, see [Chapter 10: Setting Up User Synchronization Service](#).

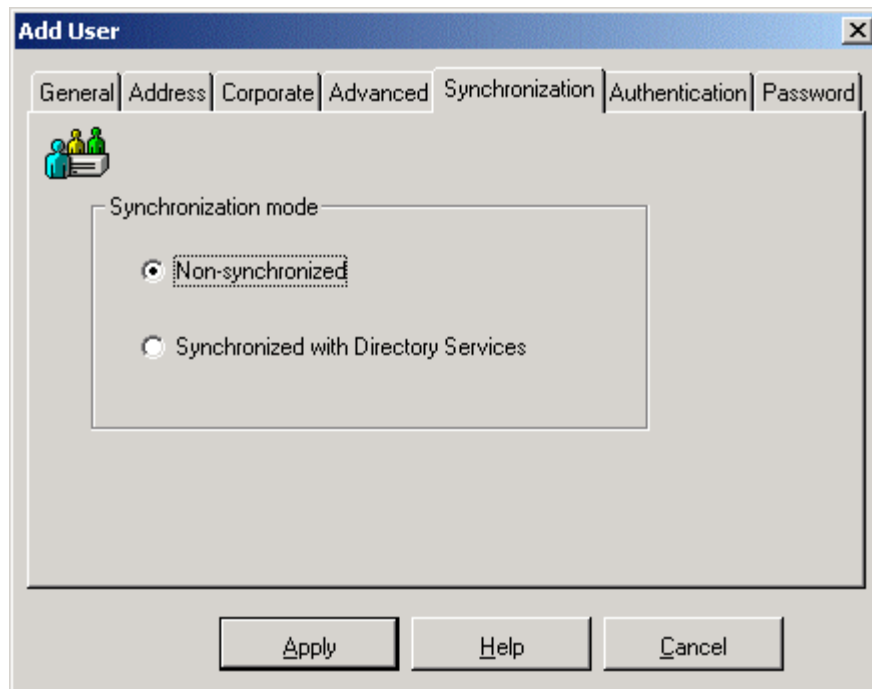


Figure 77: Add User window, setting a new user's synchronization flag

Regular and Common Users

A **regular** user is any person in your company who uses the Exigen Workflow system. Every person must have a user name and password and all other user information specified.

A **common** user is not an actual person. A common user is used to create and hold a common queue, a general place for storing documents before processing. A common user is especially useful if you have a team of people performing the same task, such as indexing documents. In this case, you can add a common user to the indexing group. When scanners send jobs to the common indexing user, any member of the indexing group can access those documents.

A common user is a special user type and must not have any security associated with it.

For information on using common users, see [Tips for Building a Workflow](#).

Specifying the Authentication Mode

Exigen Workflow provides a flexible user authentication mechanism that allows you to simplify user login to Exigen Workflow and Exigen Workflow Web. The Web server hosting the Exigen Workflow Web installation must be configured to require user login for site access. To identify users, the Web server can use the Exigen Workflow user database or it can be integrated with the Windows domain or directory.

The **Authentication** tab displays authentication modes permitted for the user.

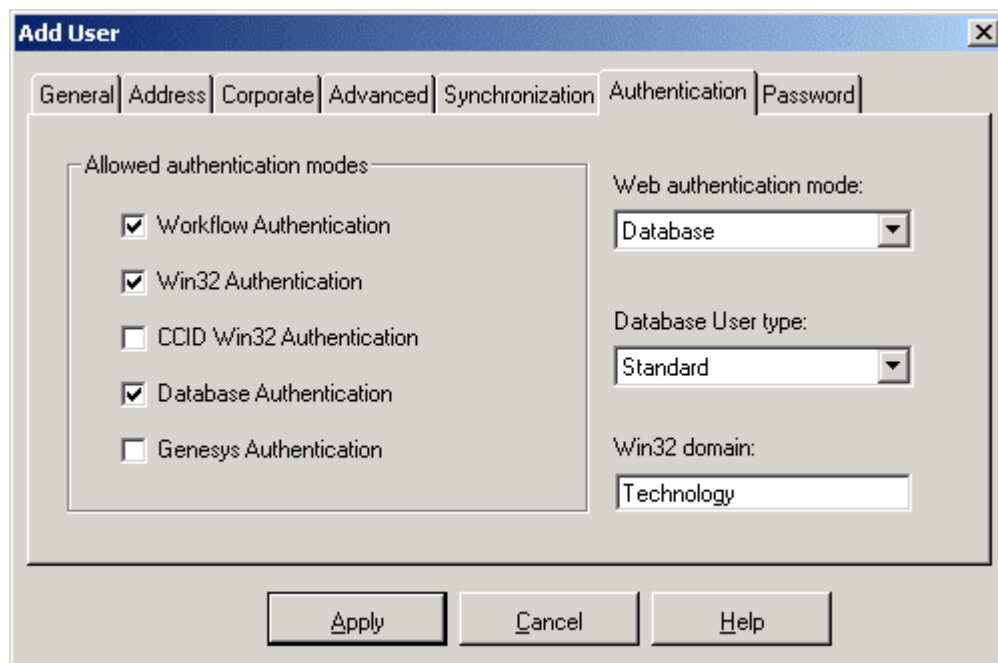


Figure 78: Add User window, setting a new user's authentication flag

Note: The **Database Authentication** option and the **Database User type** list box are available only if extended security is used.

To specify authentication mode, proceed as follows:

1. Select one or several authentication modes in Exigen Workflow and Exigen Workflow Web for a new user, based on security requirements:

Authentication mode	
Mode	Description
Exigen Workflow Authentication	User is authenticated by Exigen Workflow. This mode prompts the user to enter a login name and password in the Exigen Workflow login window.

Authentication mode	
Mode	Description
Win32 Authentication	<p>User is authenticated through the Win32 system. The mode works in Exigen Workflow Web as follows:</p> <ol style="list-style-type: none"> 1. In the Exigen Workflow Web login window, the user enters the Windows login name and password. 2. The system evaluates the user's Windows login name. If the system detects that the Exigen Workflow user's name is the same as for the Windows user, it finds the corresponding domain and attempts to authorize the user for this domain. <p>The database user type is specified by entering the Windows user and the Win32 domain names in the appropriate fields.</p>
CCID Win32 Authentication	<p>In Exigen Workflow Web, this mode is also known as Single sign-on authentication. In this mode, the user is authenticated by the current Windows user identity. This mode allows the user to work with Exigen Workflow objects without entering via the Exigen Workflow login window. The system evaluates the user's Windows login name and starts the Exigen Workflow application if this user exists in the Exigen Workflow system.</p> <p>The database user type is specified by entering the Windows user and the Win32 domain names in the appropriate fields.</p>
Database Authentication	<p>User is authenticated by the database. The database user type is specified by selecting the standard database user in the respective field.</p> <p>For information on implementing database authentication, see Database Connection Mode.</p>
Genesys Authentication	<p>User is authenticated by Exigen Workflow. This mode allows a Genesys user who is logged into a Genesys desktop application to access Exigen Workflow objects without additional Exigen Workflow authentication.</p>

Note: Genesys authentication mode is not available in Exigen Workflow Web.

The authentication mode for a client workstation in Exigen Workflow is specified in the `visiclt.ini` file located in the Windows directory. In Exigen Workflow Web, it is specified in the **Web authentication mode** database field as described in [Appendix G: Exigen Workflow User Authentication Mechanism](#).

2. In the **Password** tab, specify settings for a user password.

Figure 79: Add User window, specifying a new user's password settings

Password can expire indicates that the user password expires. The period for changing a password is specified in the **Security Settings** window as described in [Specifying Security Settings](#).

The **Password is expired** check box is enabled when **Password can expire** is selected. This setting is useful for system administrators to force users to change their passwords during the next login. If the **Password is expired** check box is selected, the newly created user is asked to change the password during the first login.

- To set the status of the user account, select one of the following **Account state** options:

Account state options	
Option	Description
Enabled	Allows the user to log in and perform all tasks in Exigen Workflow. User status is set by a system administrator.
Disabled	Prevents the user from logging in to Exigen Workflow. User status is set by a system administrator.
Value by AdSync	Enables the user status to be managed by ADSync. ADSync is a component that imports and synchronizes user accounts from an external source. During login, Exigen Workflow uses the value set by ADSync to qualify the user as disabled or enabled. For more information on user states, see ADSync Functionality .

- To unlock the user password if it is locked out by an unsuccessful login attempt, click **Unlock**.
- To specify the user password, click **Set password**.

The **Set Password** window appears.

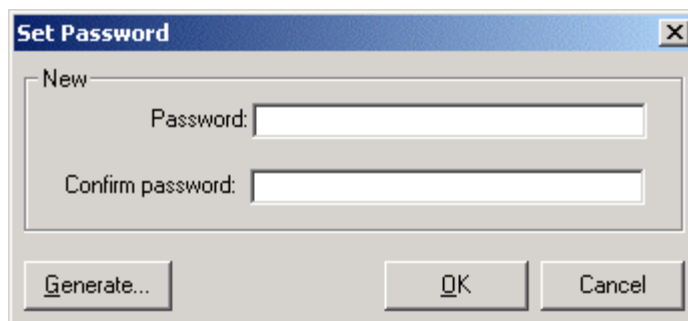


Figure 80: Set Password window

6. Enter the user password in the **Password** and **Confirm password** fields.
7. To generate a random password, click **Generate**.

The **Random Password** window appears.

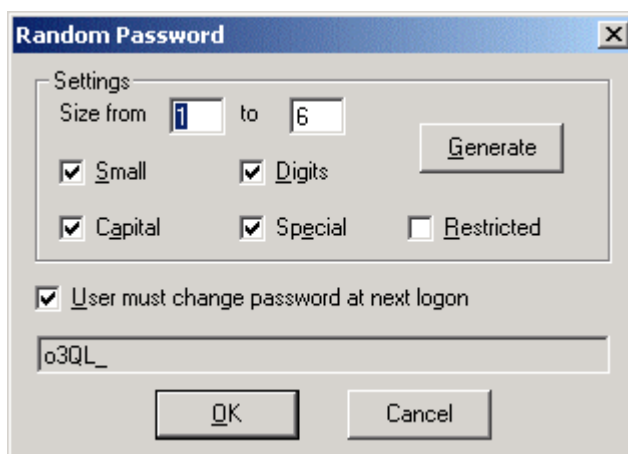


Figure 81: Random Password window

8. In the **Random Password** window, specify the parameters of the generated password.
9. To specify the minimum and maximum length of generated passwords, in the **Size from** and **to** fields, enter appropriate values.
10. To specify additional password parameters, select the appropriate check boxes described in the following table:

Random Password window check boxes	
Check box	Description
Small	Indicates that small letters are used in the generated password.
Digits	Indicates that digits are used in the generated password.
Capital	Indicates that capital letters are used in the generated password.
Special	Indicates that special characters such as * > ! ^ are used in the generated password.
Restricted	Indicates that restricted characters such as ? \ ' are used in the generated password.

Random Password window check boxes	
Check box	Description
User must change password at next logon	If selected, the newly created user must enter a new password after the first logon.

11. To create a random password, click **Generate**.
12. To save the password settings, in the **Set Password** window, click **OK**.
13. Once all tabs are filled in, to add the user to the list, click **Apply**.

The newly created user must be added to a user group in the workflow group setup.

For information on workflow group setup, see [Setting Up Workflow Groups](#).

14. To change user attributes, select the user and click **Modify**.
15. To delete the user from the system, select the user and click **Delete**.

Specifying Document Types a User Can Access

A **document type** classifies and identifies a document, and protects it against unauthorized use. In Exigen Workflow, document types are stored as records in a separate table named **DOCTYPES**, which is used as a reference table for each document record so that only those document types specified in the DOCTYPES table can be chosen for any document.

Note: For a newly created project, no document types are specified. Document types are defined using the Table Maintenance tool, as described in [Project Table Maintenance](#).

The **Document Types** tab in the **User Setup** window allows or denies user access to a specific document type.

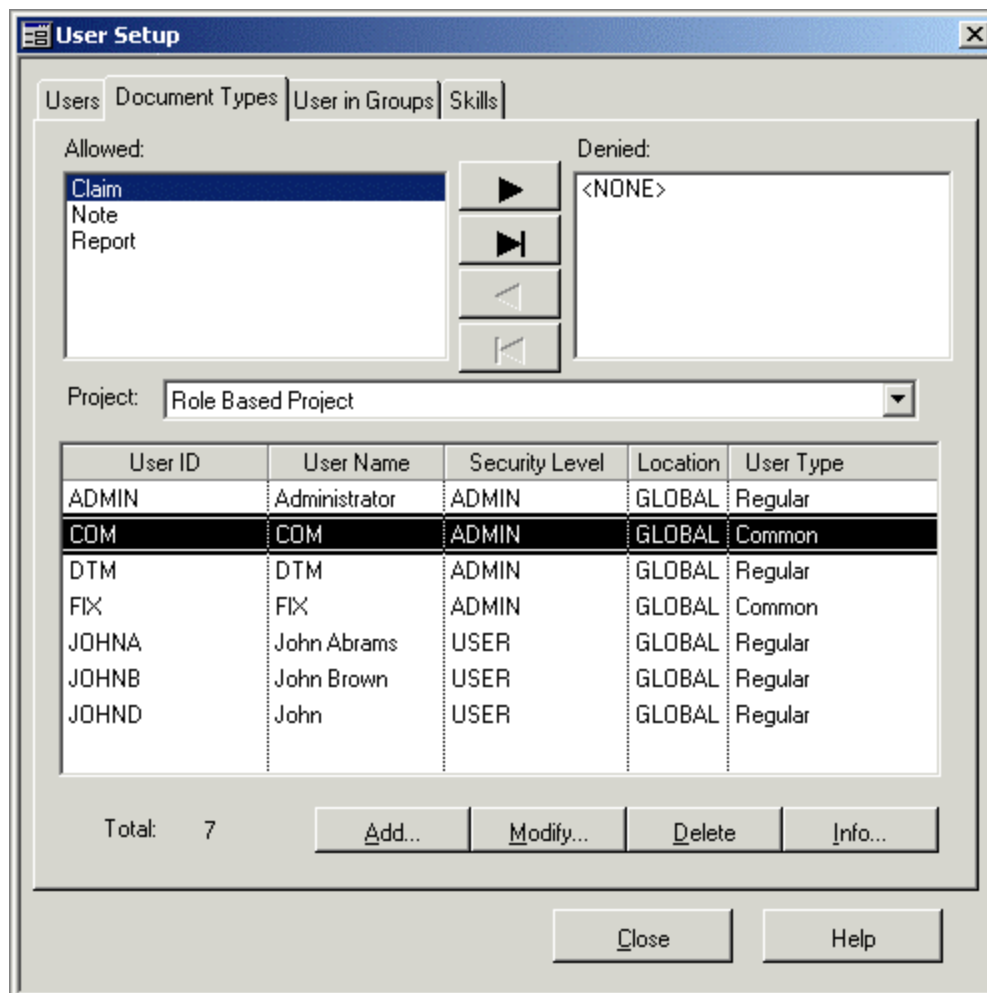


Figure 82: User Setup window, Document Types tab

The **Allowed** list shows the document types that can be accessed by the user. The **Denied** list shows the document types denied to the user.

Move document types from left to right and right to left into the desired list by clicking the following buttons:

- **Move Right**
- **Move All Right**
- **Move Left**
- **Move All Left**

Setting Up Tasks

Task Objects are external applications, such as Word or Notepad that can run from inside Exigen Workflow objects. You can attach the same task object to many workflow objects and create many task objects for the same external application.

The following topics are included in this section:

- [Setting Up Tasks](#)
- [Setting Up Document Templates for Tasks](#)
- [Specifying a Default Document Type for a Task](#)

Setting Up Tasks

To set up tasks, proceed as follows:

1. Click **Tasks Setup**.



The **Task Setup** window appears.

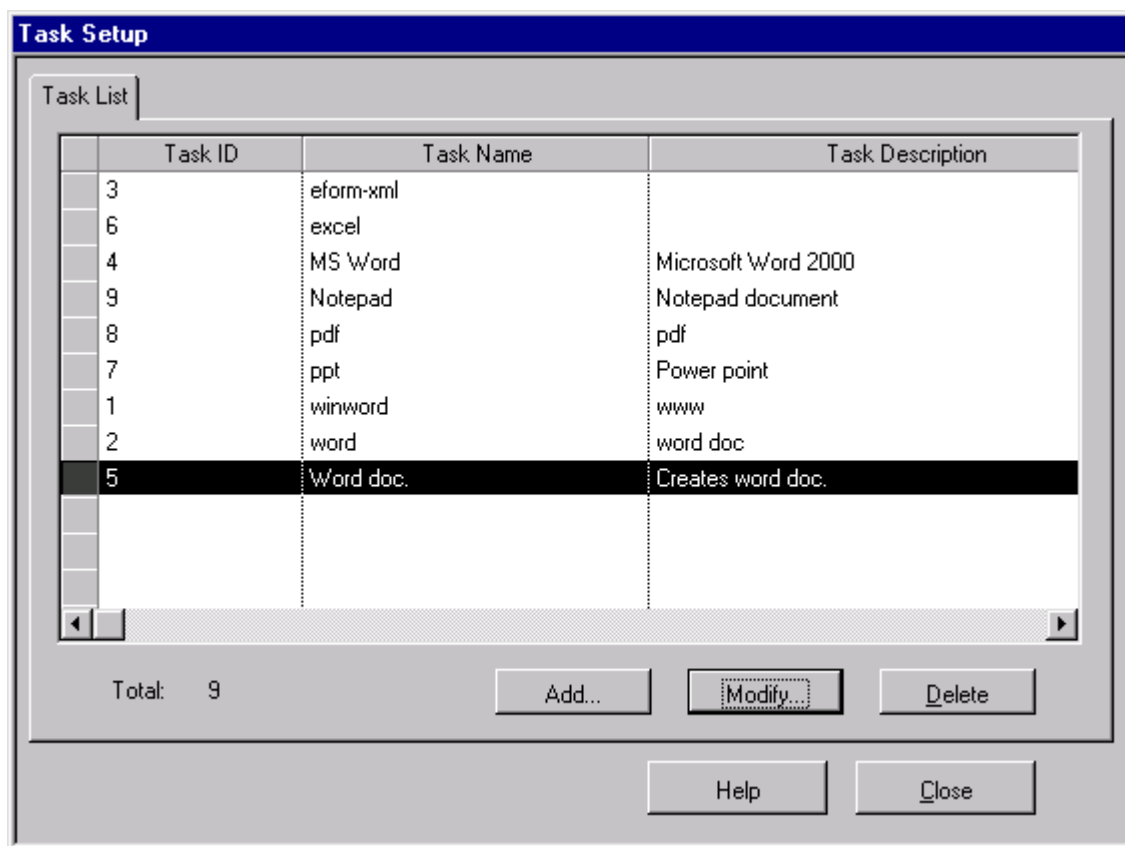


Figure 83: Task Setup window

The **Task List** tab displays the task ID, which is assigned by the system, the task name and the task description.

2. To add a task, click **Add**.

The **Add Task** window appears.

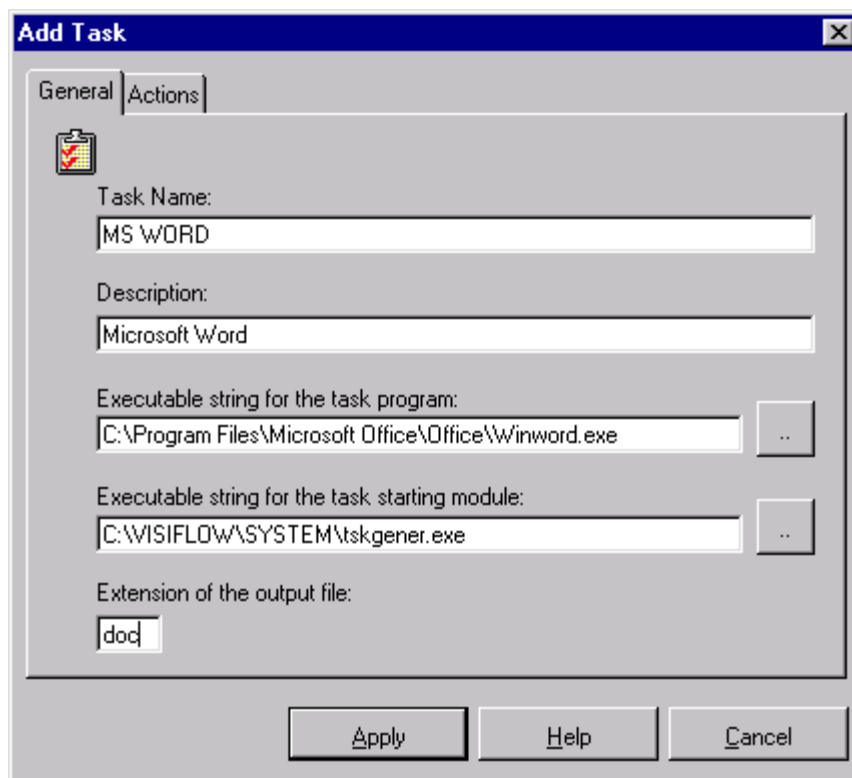


Figure 84: Add Task window, General tab

3. In the **General** tab, enter values in the following fields:

Add Task window, General tab	
Field	Description
Task Name	Task object name. This identifies the task for the Exigen Workflow system and the user.
Description	Task description.
Executable string for the task program	Task executable location, such as WINWORD.EXE or EXCEL.EXE. The path to the task executable cannot exceed 60 characters.
Executable string for the task starting module	TSKGENER.EXE file location in the Exigen Workflow system directory. The path to the task starting module cannot exceed 60 characters.
Extension of the output file	Three-letter extension.

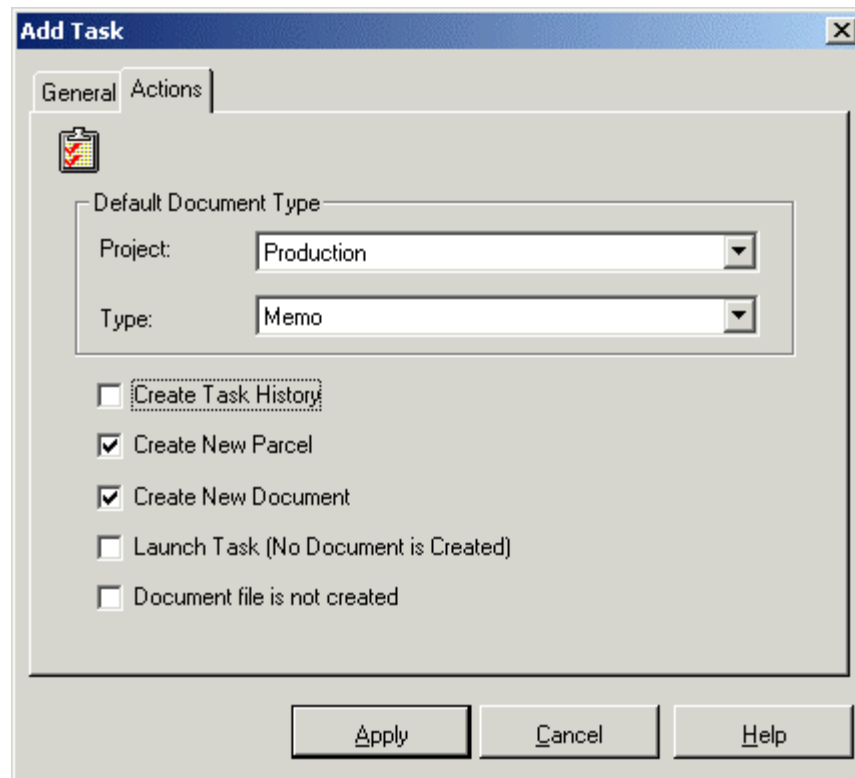


Figure 85: Add Task window, Actions tab

4. In the **Actions** tab, configure parameters described in the following table:

Add Task window, Actions tab	
Parameter	Description
Project	Project containing the document types for this task.
Type	Default document type. The document type is assigned by default to all documents created by this task. For a newly created project, no document types are specified. The Table Maintenance tool is used to define the document types for the project as described in Project Table Maintenance . If no type is selected, new documents are created without a document type.
Create Task History	Creates a task history record.
Create New Parcel	New parcel is created in which to place the completed task.
Create New Document	Completed task is placed in the same parcel as the new document.
Launch Task (No Document is Created)	Only the application is launched.
Document file not created	Document is not created when using an external application that normally creates one.

One or more actions can be assigned to a task.

A defined task can be assigned to a node as described in [General Tab](#). Tasks can be assigned to all workflow nodes, but restrictions on task actions in nodes apply as described in [Restrictions on Task Actions in Nodes](#).

Setting Up Document Templates for Tasks

Document templates are draft documents created in an external application such as Word or Excel. Document templates are assigned to projects containing tasks.

For example, if the task is named Prepare invoice, and it is associated with Word, an invoice template is created as a Word document and is assigned to the project. When the user starts the task and selects the appropriate document type, the template is displayed.

Note: This feature is not available in standard Exigen Workflow client/server and Web applications. It is supported by programmable extensions only, and is available via application programming interfaces (APIs). For information on how to acquire this feature, contact Exigen Support Services.

To set up document templates, proceed as follows:

1. Ensure that a task is set up for the appropriate workflow node.

For information on setting up tasks, see [Setting Up Tasks](#).

2. Ensure that subfolders are set up for the project as described in [Project Table Maintenance](#).
3. Ensure that document types are set up for the project as described in [Maintaining Project Tables](#).
4. Specify a default document type for the task as described in [Specifying a Default Document Type for a Task](#).
5. Prepare a document template and save it on the computer where Exigen Workflow is installed.
6. Use Template Management Utility to assign the template to the appropriate Exigen Workflow project as described in the *Exigen Workflow Administrator's Guide, Part 3: Utilities, Chapter 8: Template Management Utility*, Assigning a Document Template to a Project.

For information on accessing and using the document template, see the *Exigen Workflow User's Guide*, Chapter 7: Queue Processing, Opening a Document Template.

Specifying a Default Document Type for a Task

A default document type is specified for a task to help the user select the appropriate document template when starting the task.

To specify a default document type for a task, proceed as follows:

1. Open the **Administrator** tool as described in [Setting Up the System](#).
2. Select **Administrator > System Setup**.
3. Click **Tasks Setup**.
4. Select the task and click **Modify**.

The **Modify Task** window appears.

5. Select **Actions**.

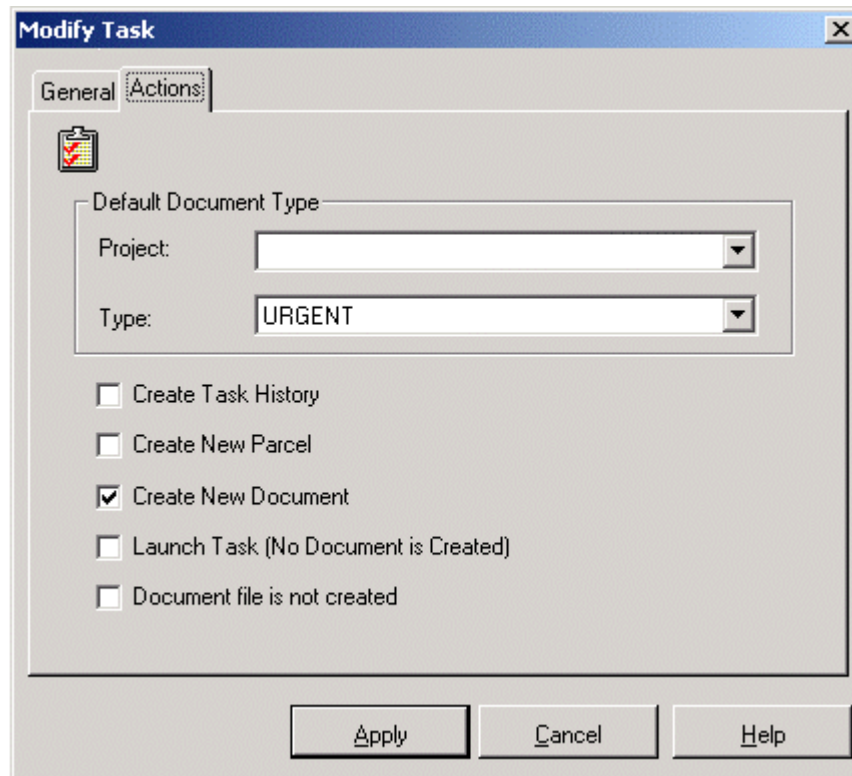


Figure 86: Specifying a default document type

6. Select the **Create New Document** option.

If the **Create New Document** option is not selected, a document type cannot be assigned.

7. In the **Project** list box, select the project.
8. In the **Type** list box, select the document type.
9. To save the settings and close the window, click **Apply**.

Setting Up Events

Events are automatic processes.

In previous Exigen Workflow versions, events were processed by Advanced Event Server.

Advanced Event Server is replaced by Automatic Queue Server, and Automatic Queue Server handlers can be set up to process events. It is recommended that synchronous parcel processing is used. For more information on Exigen Workflow handlers, see the *Exigen Workflow Administrator's Guide, Part 2: Business Component Reference*, Chapter 21: Exigen Workflow Handlers.

You can set up the system to trigger different actions when users perform different types of transactions. In Event Setup, all possible events and the types of data required to perform a function are defined. Events must reflect actual functions set up in Exigen Workflow. For more information on events, see [Exigen Workflow Events](#) in [Chapter 5: Designing a Workflow](#).

To set up events, proceed as follows:

1. Click **Workflow Event Setup**.



The **Workflow Event Setup** window appears.

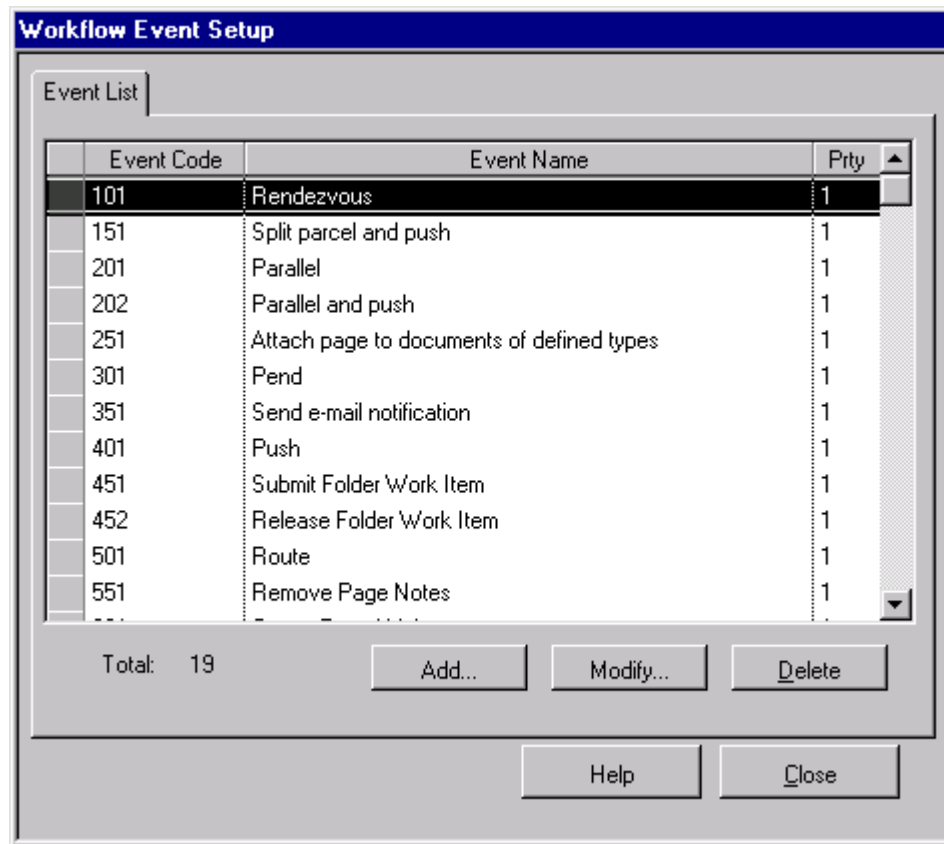


Figure 87: Workflow Event Setup window

The window displays the event code that is used to perform the action, the event name, and the priority.

2. To add an event, click **Add**.

The **Add Event** window appears.

Figure 88: Add Event window

3. To define an event, in the **General** tab, enter values in the following fields:

Add Event window, General tab	
Value	Description
Event Code	<p>Value provided by Exigen. Only the codes registered in Automatic Queue Server are executed.</p> <p>Standard Centura events have the following values: 101, 151, 201, 202, 251, 301, 351, 401, 451, 452, 501, 551, 601, 701, 702, 801, 901, 902.</p> <p>Custom Centura events have the following values: 1-16, 1001-1004, 2001-2006, 3001, 4001.</p> <p>There is also an internal workflow event 999999999.</p>
Event Name	Name used to identify this event.
Event Description	Description of the processes the event performs.
Priority	<p>Order in which each event is processed. Priority is set to 1 if no number is entered.</p> <p>Note: Priority value is not currently used by Automatic Queue Server.</p>
Parameter Description	Required event parameters description. These parameters are provided by Exigen.

4. To change an event, select it and click **Modify**.
5. To delete an event, select it and click **Delete**.

Managing Stamps

Stamps are electronic images of actual rubber stamps applied to document images.

Stamps are created with the Stamp Utility. After they are created, you can assign users the rights to apply them to document images.

To manage stamp security, proceed as follows:

1. Click **Stamps Setup**.



The **Stamps Setup** window appears.

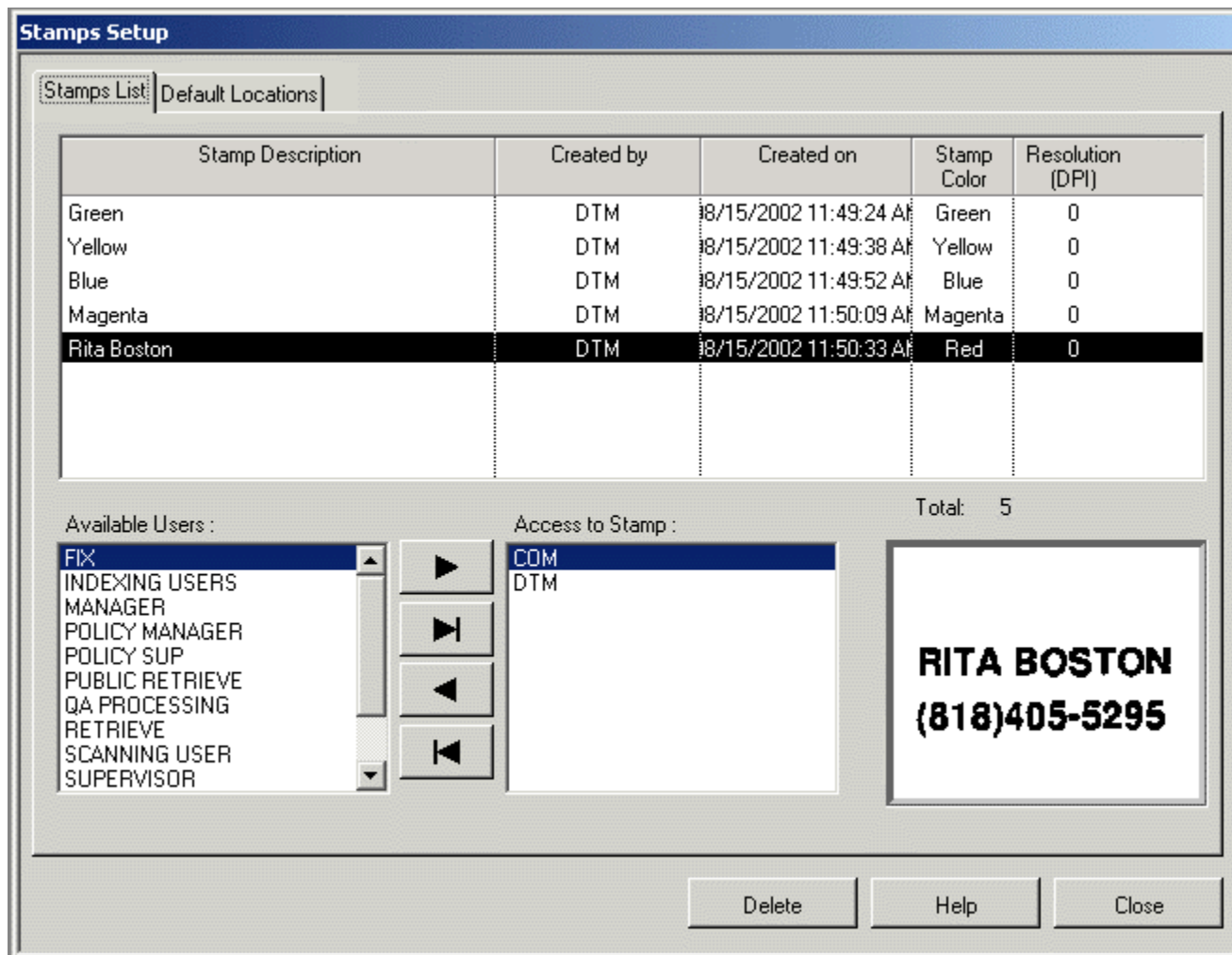


Figure 89: Stamps Setup window

A table in the upper part of the window lists rubber stamps in your system. The image of the rubber stamp is displayed in the lower right pane.

2. To allow or restrict the stamp to certain users, click the following buttons:

- **Move Right**
- **Move All Right**
- **Move Left**
- **Move All Left**

Note: Only a user who has placed a stamp on an image is allowed to delete or move the stamp.

3. To specify location settings for stamps and document types, select the **Default Locations** tab.

The **Default Locations** tab is used to add, modify, and delete location settings.

4. To add a new location setting, click **Add**.

5. The **Add Default Stamp Location** dialog appears.

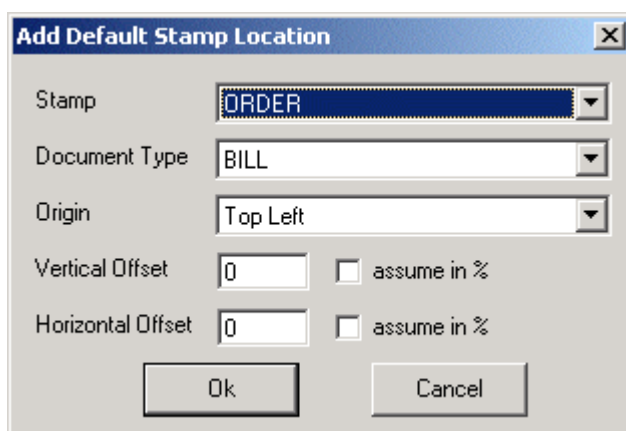


Figure 90: Add Default Stamp Location window

Specify the following settings for a new location:

Add default Stamp Location window settings	
Field	Description
Stamp	List of available stamps.
Document Type	List of available document types.
Origin	Origin location for a stamp.
Vertical Offset	Vertical offset of a stamp in a document from the origin.
Horizontal Offset	Horizontal offset of a stamp in a document from the origin.

Offsets are calculated as the distance from the origin to the nearest stamp border. Offsets also can be specified as percentages of document dimensions. For example, if you need a stamp located at lower right, but 10% higher, the distance from the bottom of the document to the bottom of the stamp is 10% of document height. In this example, you set **Vertical Offset** to *10* and select **assume in %**. By default, offsets are calculated in pixels.

- When the stamp definition is completed, add this stamp to your document using the **Stamp** menu in Image Viewer.

If a document is assigned to a document type and there is a row in the stamp location table with this document type and a stamp, a stamp is placed in the defined location. Otherwise, the stamp appears in the top left corner.

Setting Up Locations

The **Locations Setup** defines storage locations for workflow scripts, form templates, and electronic rubber stamps.

To define storage directories, proceed as follows:

- Click **Locations Setup**.



The **Locations Setup** window appears.

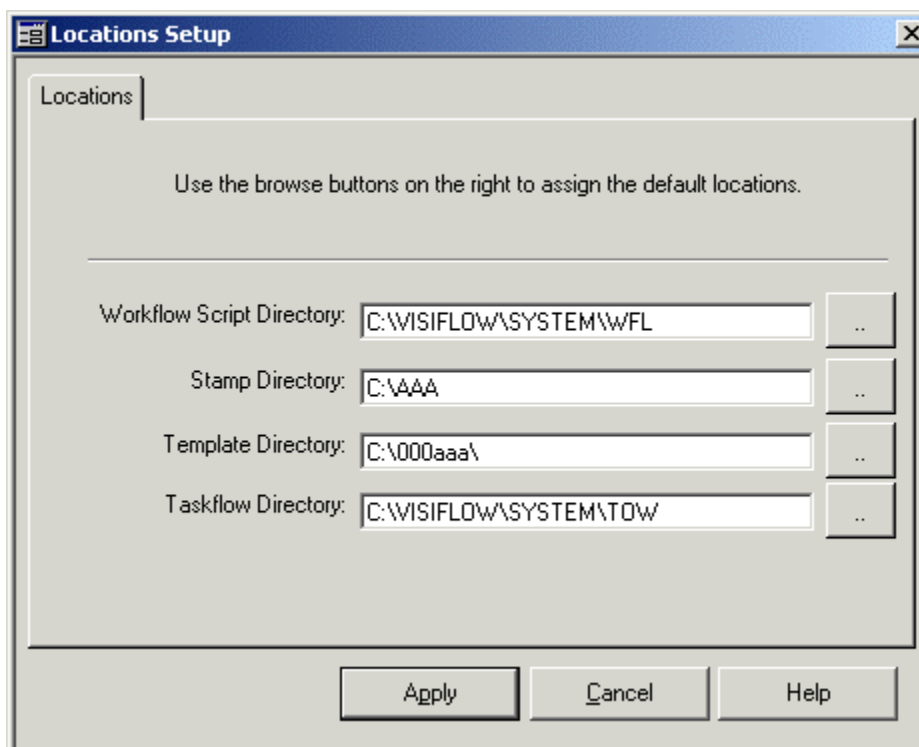


Figure 91: Locations Setup window

- To define locations, in the **Locations Setup** window, click the browse buttons next to the fields.

The following table describes the fields in the **Locations Setup** window:

Locations Setup window fields	
Field	Description
Workflow Script Directory	Location of workflow scripts created each time the workflow is saved.
Stamp Directory	Location of all electronic stamps created using the Stamp Utility.
Template Directory	Location of all form and EDI templates created using the Template Maintenance Utility.
Taskflow Directory	Location of task checklist text files, interaction scripts, Automatic Queue Server scripts, and other configuration files used for tasks in Task Oriented Workflow.

3. When all directories are located, to save changes, click **Apply**.

Warning: The system allows you to specify only one location, or path, for each database. If there are several projects in a database, they all use the same storage locations.

Setting Up Global User Groups

Global user groups and document context security levels provide DMS document annotation security in the Exigen Workflow system. Users are able to either view or edit specific private annotations based on access rights. Users having no access rights for the private annotation cannot view the annotation on the document.

A **global user group** is a list of users or user groups. Global user groups are used to define document context security levels. For information on document context security levels, see [Setting Up Document Context Security Levels](#).

Global user groups are also used to organize users in ACL based security.

There are the following types of global groups:

Global group types	
Type	Description
Standard	Global groups in which users must be added manually.
Automatic	Global groups in which users are maintained automatically based on user properties.

To maintain global user groups, proceed as follows:

1. In the **Administrator Utilities** window, click **System Setup**.



2. In the **System Setup** window, click **Global User Groups Setup**.



The **Global User Groups** window appears.

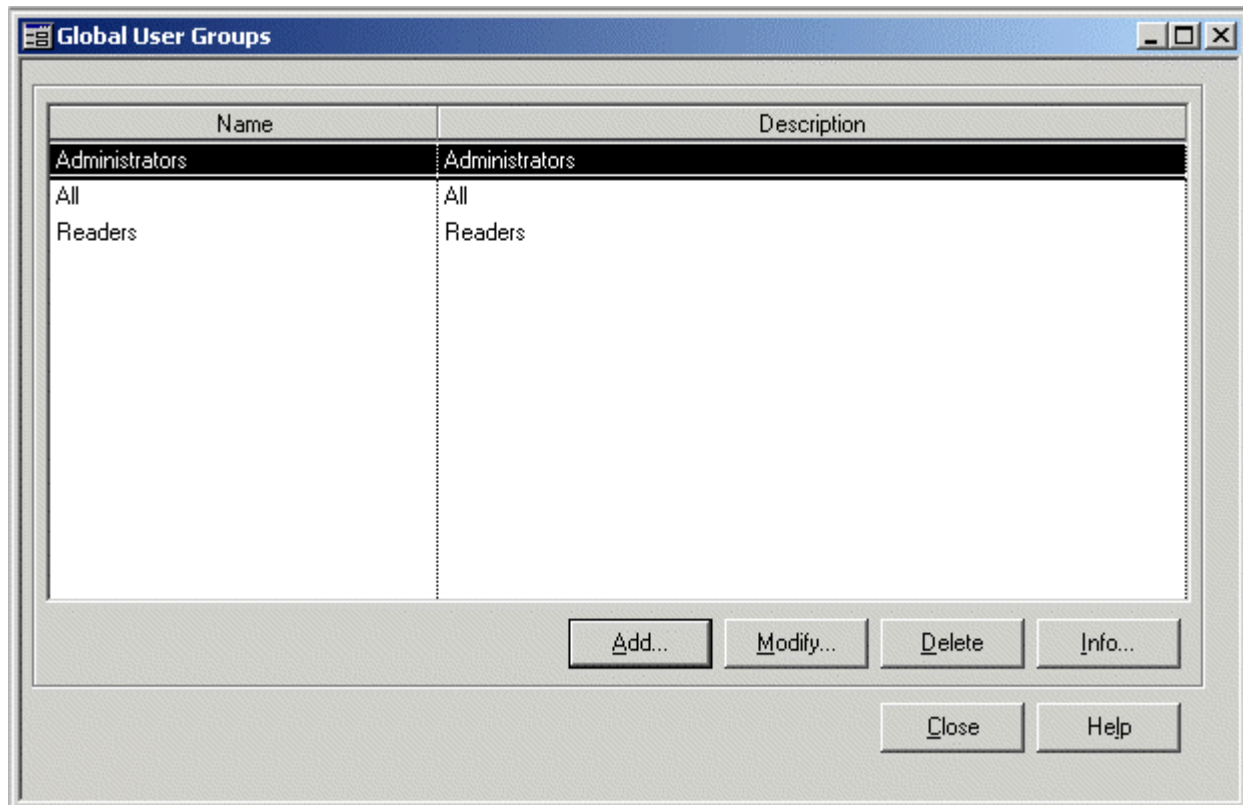


Figure 92: Global Users Groups window

The **Global Users Groups** window displays the existing global user group names and descriptions.

3. In the **Global Users Groups** window, perform the following tasks as required:

- [Adding a Global User Group](#)
- [Modifying a Global User Group](#)
- [Deleting a Global User Group](#)
- [Viewing a Global User Group Definition](#)

Adding a Global User Group

To add a global user group, proceed as follows:

1. Click **Add**.

The **Global Group** window appears.

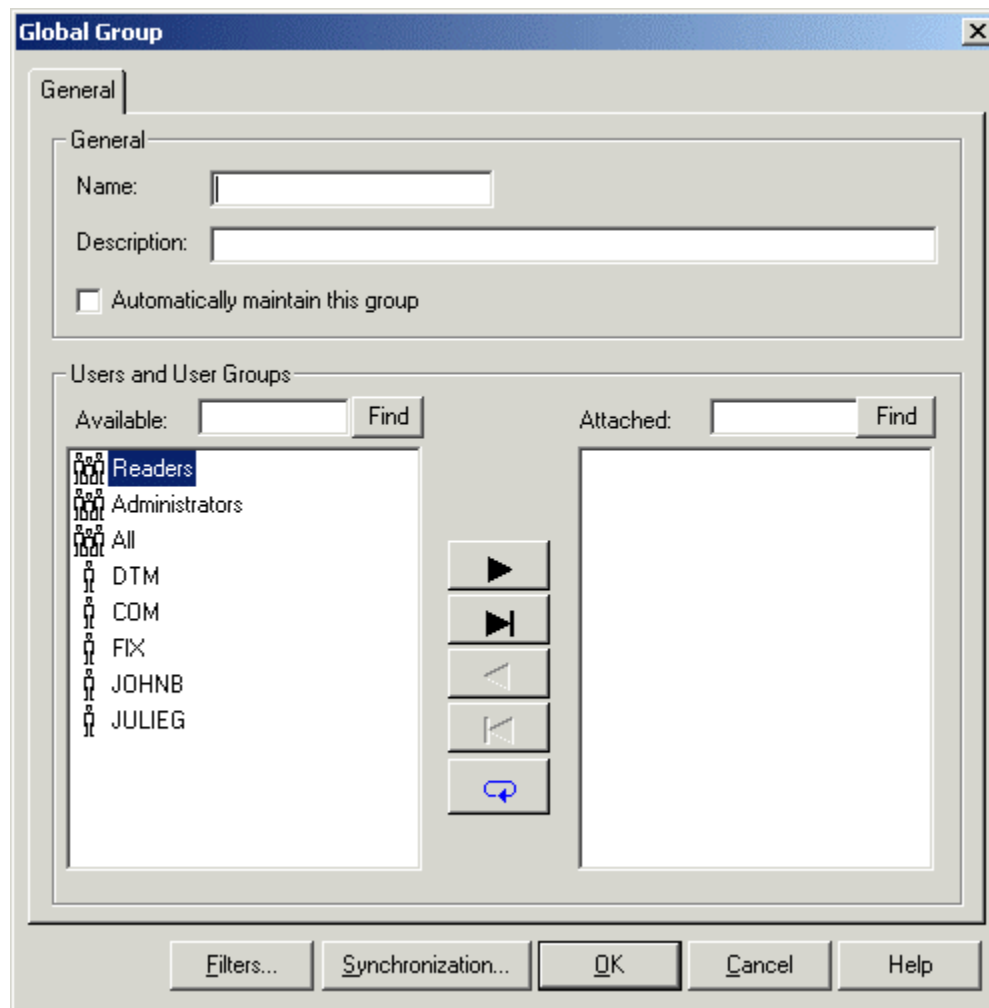




Figure 93: Global Group window

2. Enter a global group name and description.

The name must be unique and descriptive.

3. To add a user, select the user name in the left list, and click **Add User** .

4. To add all users to the group, click **Add All Users** .

5. To remove a user, select the user name in the list on the right, and click **Remove User** .

6. To remove all users and groups from the group, click **Remove All** .

7. To search for a specific user who is not already assigned to the group, in the **Available** field, enter the user's name and click **Find**.

8. To search for the assigned user, in the **Attached** field, enter the user's name and click **Find**.

9. To automatically maintain users in the global group, select the **Automatically maintain this group** check box.

If the **Automatically maintain this group** check box is selected, users are automatically added or removed from the global group based on global group filters. For information on global group filters, see [Defining Global Group Filters](#).

10. To define the global group filters, click **Filters** and follow the instructions as described in [Defining Global Group Filters](#).
11. To synchronize the global group with an external domain group using ADSync, click **Synchronization**, and, in the **Synchronization Setup** window, enter the synchronization information used by ADSync.
12. To save the settings, click **OK**.

Defining Global Group Filters

Global group filters define the criteria for users to be added to the group. When a new global group is created, all users are checked for accordance to the global group filters and are automatically added to the group if the user properties match the filters.

If the group is automatic, all users in it are maintained based on the global group filters. If user properties match the group filters, the user is automatically added to the group. If a user is added to the group but its properties do not match the group filters, the user is automatically removed from the group. User group membership is verified only when users are added, modified, or deleted in the system.

To define global group filters, proceed as follows:

1. In the **Global Group** window, click **Filters**.

The **Filters** window appears.

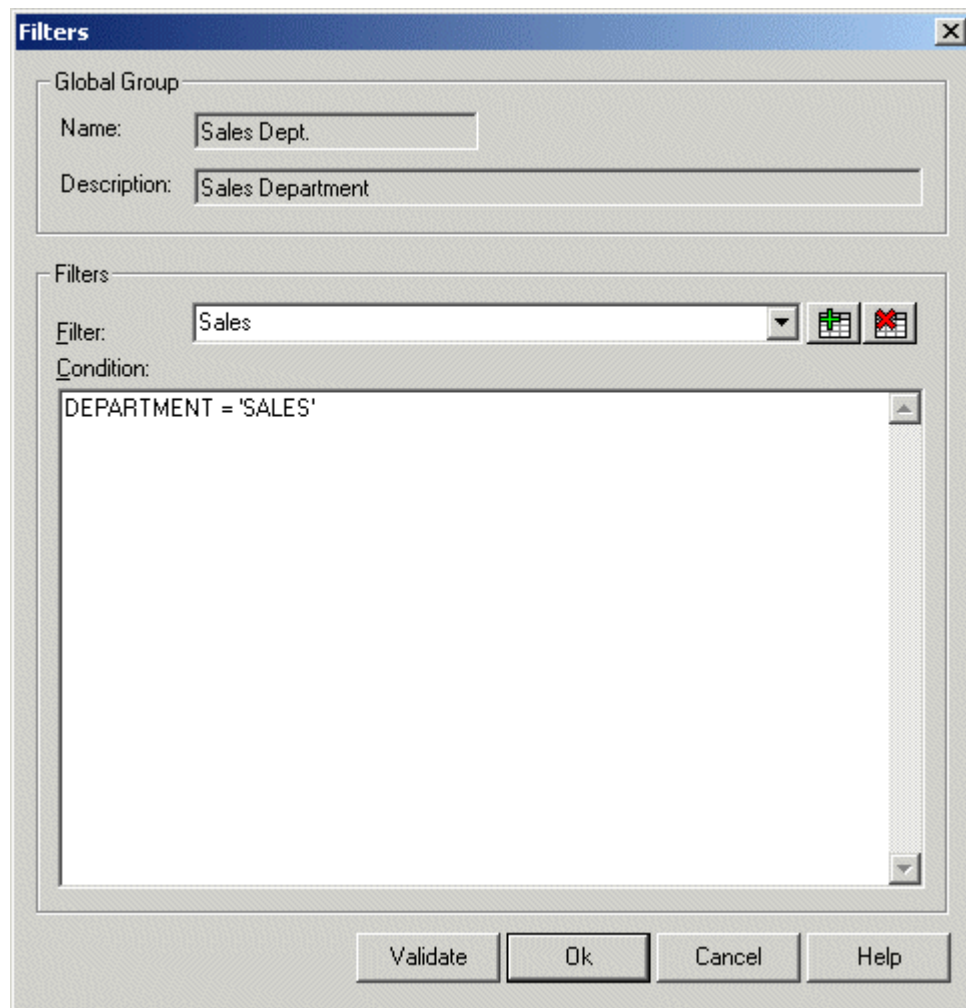


Figure 94: Configuring global group filters

The **Global Group** box displays the group information.

2. To add a new filter, click **Add New Filter**.

The **Filter Name** window appears.

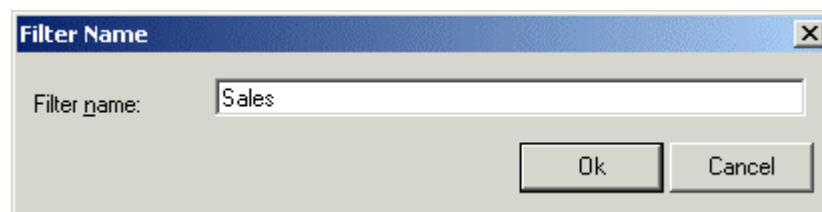


Figure 95: Adding a filter

3. In the **Filter** name field, specify a descriptive name for the new filter.
4. Click **Ok**.
5. In the **Condition** field, enter a standard SQL statement defining the criteria for users in the group.

The defined SQL statement is added to the WHERE operator during the global group query. The statement must reference only fields from the S01_USERS table.

6. To delete a filter, click **Delete Filter**.
7. To verify that the filter condition is valid, click **Validate**.
8. If an error message appears, correct the condition statement and click **Validate** again.
9. If the statement is correct, click **OK**.

The confirmation window appears.

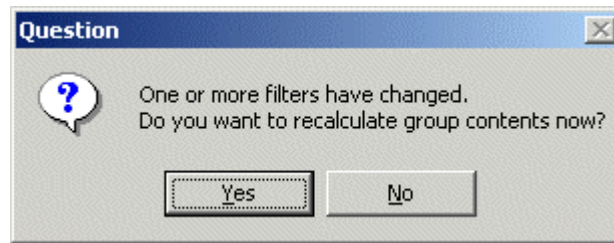


Figure 96: Confirmation window

10. To recalculate the users in the global group, click **Yes**.

Modifying a Global User Group

To modify the group's name, description, and assigned users, proceed as follows:

1. In the **Global User Groups** window, select the global user group and click **Modify**.

The **Global Group** window appears showing the selected group.

2. Modify the group's name and description.
3. To save the changes, click **OK**.
4. To reassign users, perform the steps described in [Adding a Global User Group](#).

Deleting a Global User Group

To delete a global user group, proceed as follows:

1. In the **Global User Groups** window, select the global user group and click **Delete**.

The confirmation window appears asking to confirm group deletion.

2. To delete the group, click **Yes**.

The global user group is deleted from the system.

Viewing a Global User Group Definition

To view a global user group definition, select the global user group and click **Info**.

The **Global Group** window appears showing the selected group in read-only mode.

Setting Up Document Context Security Levels

A document context security level specifies a group of users who have the same security rights for document context operations such as highlighting and adding posted notes.

To specify a document context security level, click **Document Context Security Levels Setup**.



The **Document Context Security Levels** window appears.

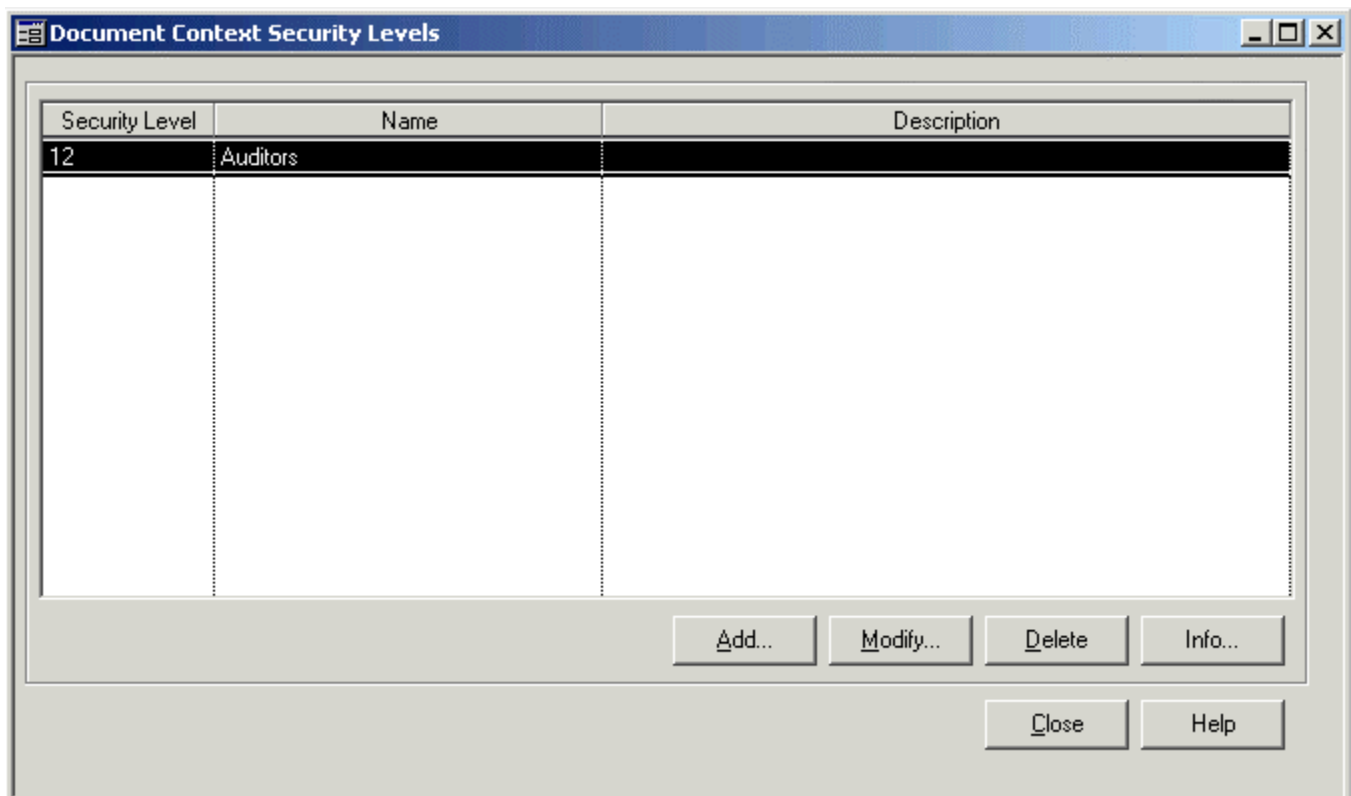


Figure 97: Document Context Security Levels window

The **Document Context Security Levels** window displays the existing security level identifiers, names, and descriptions.

Perform the following tasks in the **Document Context Security Levels** window:

- [Adding a Document Context Security Level](#)
- [Modifying a Document Context Security Level](#)
- [Deleting a Document Context Security Level](#)
- [Viewing a Document Context Security Level Definition](#)

Adding a Document Context Security Level

To add a document context security level, proceed as follows:

1. In the **Document Context Security Levels** window, click **Add**.

The **Document Context Security Level** window appears.

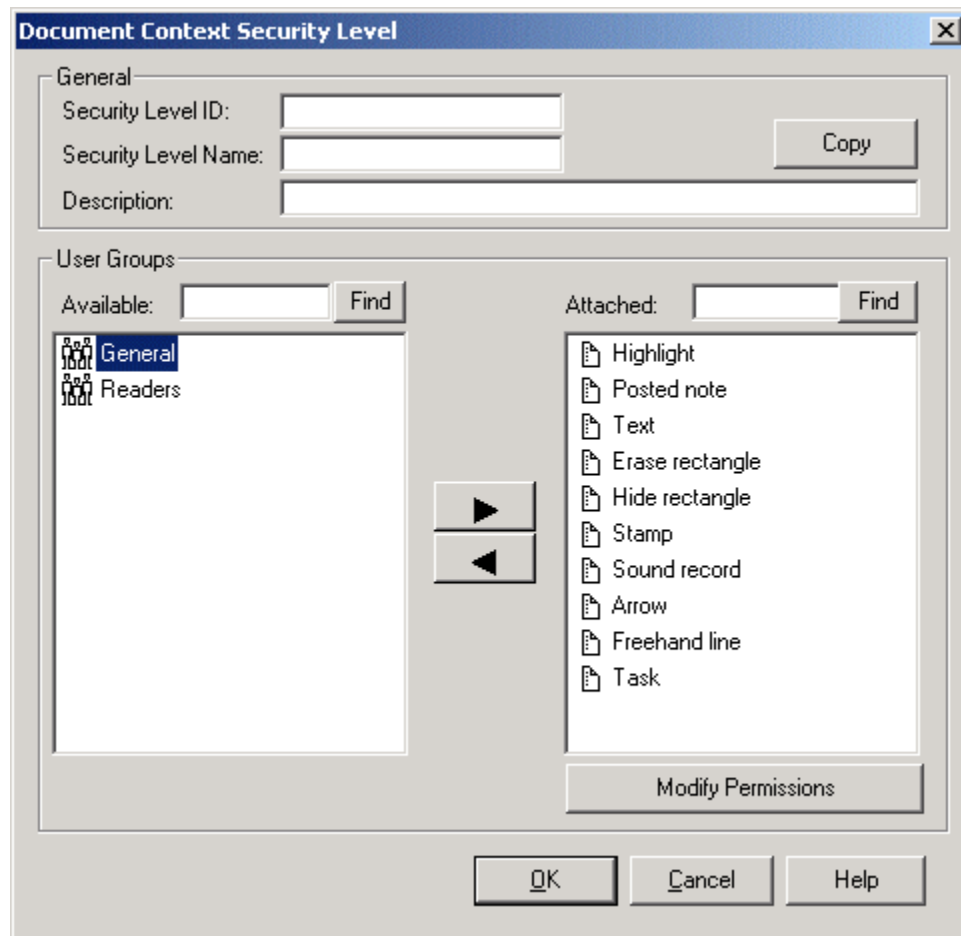



Figure 98: Document Context Security Level window

2. In the **General** section, enter a security level identifier, name, and description.

The identifier must be unique. The name must be unique and descriptive.

3. To assign permissions, select the global group in the left list and click **Add Permission** .

The **Assign/Modify permissions** window appears.

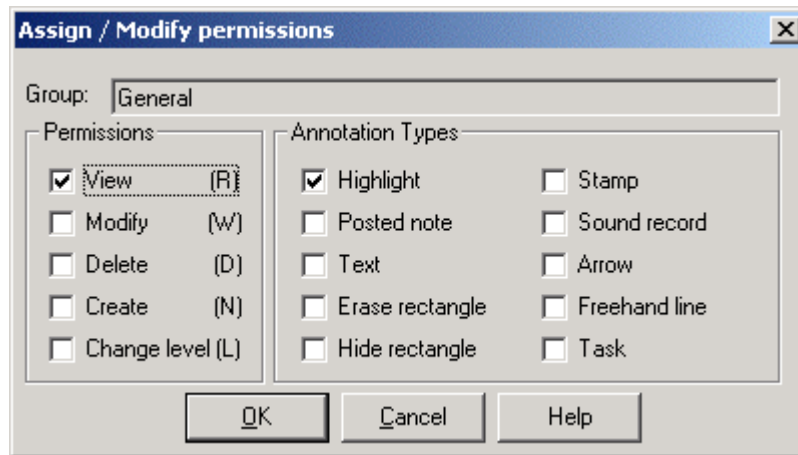


Figure 99: Assign/Modify permissions window

The **Assign/Modify permissions** window displays the existing Exigen Workflow annotation types and permissions. The selection of **Change Level** provides the possibility to change the assigned security level. For more information on annotations, see the *Exigen Workflow User's Guide*, Chapter 11: Image Viewer, Annotating Document Images.

4. Select the desired annotation types and permissions.
5. To apply the settings, click **OK**.

The assigned permissions appear in the **Document Context Security Level** window.

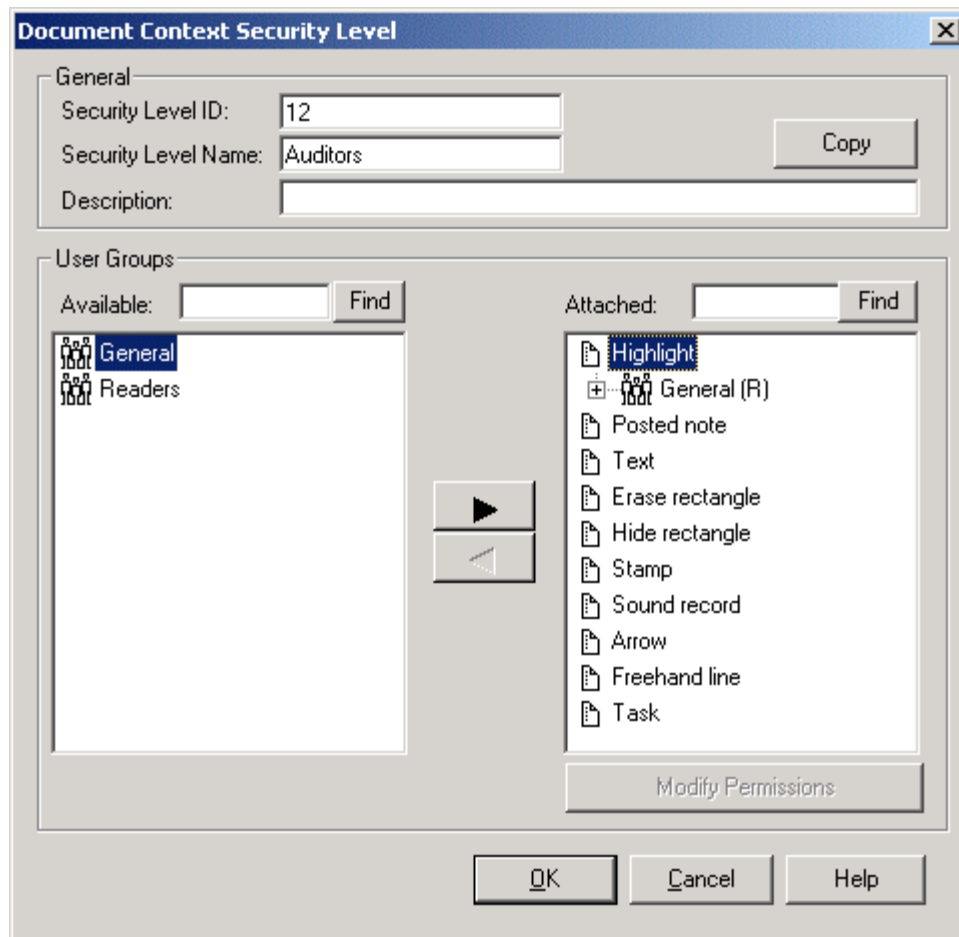



Figure 100: Assigned permissions for annotations

6. To modify the assigned permission, select the permission in the list on the right and click **Modify Permissions**.

The **Assign/Modify permissions** window appears with the enabled permissions.

7. Select or clear the desired permissions.
8. To remove the assigned permission, select the permission in the list on the right, and click **Remove Permission** .

The permission is removed from the list on the right.

9. To search for a specific user that is not already assigned to the group, enter the user's name in the **Available** field and click **Find**.
10. To search for the assigned user, enter the user's name in the **Attached** field and click **Find**.
11. To copy the specified level permissions, click **Copy**.

The **Document Context Security Levels** window appears.

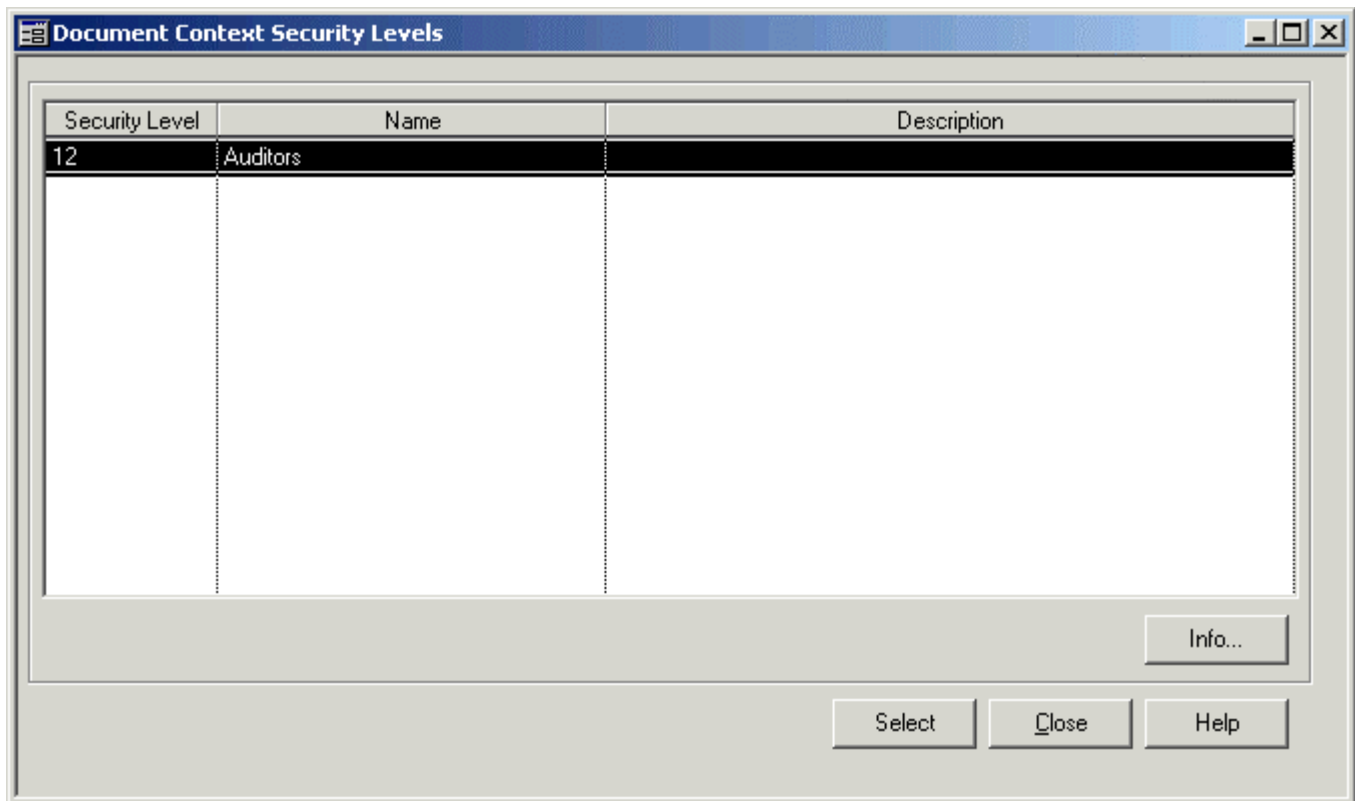


Figure 101: Selecting a document security level to copy

12. Select the security level and click **Select**.

The permissions appear in the list on the right.

13. To save the settings, click **OK**.

Modifying a Document Context Security Level

To modify the existing document context security level identifier, name, description, and assigned permissions, proceed as follows:

1. In the **Document Context Security Levels** window, click **Modify**.

The **Document Context Security Level** window appears.

2. Modify the document context security level identifier, name, and description.
3. Reassign permissions.
4. To save the changes, click **OK**.

For information on document context security levels, see [Adding a Document Context Security Level](#).

Deleting a Document Context Security Level

To delete a document context security level, proceed as follows:

1. Select the level and click **Delete**.

The confirmation window appears asking to confirm level deletion.

2. To delete the level, click **Yes**.

The level is deleted from the system.

Viewing a Document Context Security Level Definition

To view a document context security level, select the security level and click **Info**.


The **Document Context Security Levels** window appears, showing the selected level in the read-only mode.

Setting Up Document Types

This section describes how set up document types and how to associate them with document templates.

Note: The document types feature is not available in standard Exigen Workflow client/server and Web applications. It is supported by programmable extensions only, and is available via application programming interfaces (APIs). For information on how to acquire this feature, contact Exigen Support Services.

To set up document types, proceed as follows:

1. In the **System Setup** window, click **Document Types Setup** .

The **Project Document Types Setup** window appears.

2. In the **Project** field, select the required project.

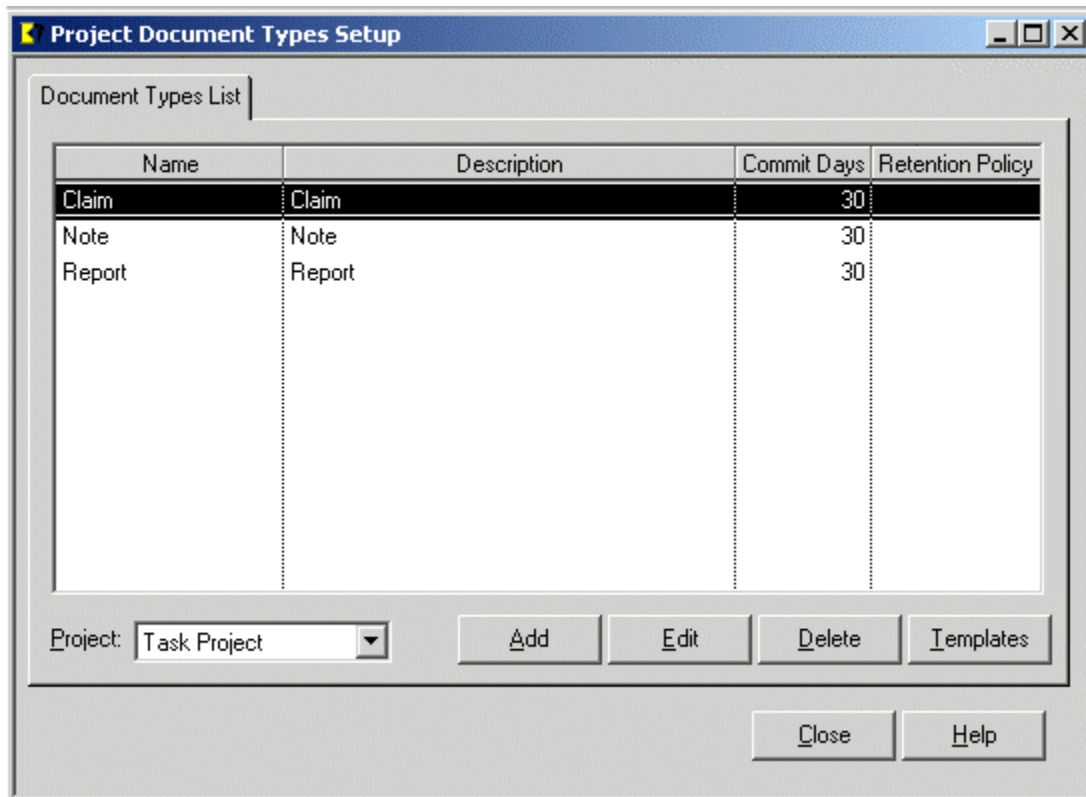


Figure 102: Setting up document types

The **Project Document Types Setup** window displays the names, descriptions, commit days, and assigned retention policies for existing document types in the selected project.

3. In the **Project Document Types Setup** window, perform the following tasks as required:
 - [Adding a Document Type](#)
 - [Modifying a Document Type](#)
 - [Deleting a Document Type](#)
 - [Associating Document Templates](#)

Adding a Document Type

To add a document type, proceed as follows:

1. In the **Project Document Types Setup** window, click **Add**.

The **Add Document Type** window appears.

Field Title	Value
Document Type	<input type="text"/>
Document Type Description	<div></div>
Default days till commit	
Retention instructions ref.	

OK Cancel

Figure 103: Adding the document type

- In the fields, enter the appropriate values as described in the following table:

Add Document Type window fields		
Name	Description	Example
Document Type	Document type name.	Claim
Document Type Description	Document type description.	Client claim on service
Default days till commit	Days until the document type must be inspected.	30

The **Retention instructions ref.** field displays the related retention policy name. The value in this field cannot be modified. For information on retention policies, see *Administrator Guide, Part II*, Chapter 12: Document Retention.

Custom document type fields can be added as described in [Project Table Maintenance](#).

- To save changes, click **OK**.

Modifying a Document Type

To modify existing document types, proceed as follows:

- In the **Project Document Types Setup** window, select a document type.
- Click **Edit**.

The **Modify Document Type** window appears.

- Modify the document type field values as described in [Adding a Document Type](#).

Deleting a Document Type

To delete a document type, proceed as follows:

1. In the **Project Document Types Setup** window, select a document type and click **Delete**.

The confirmation window appears, asking you to confirm the type deletion.

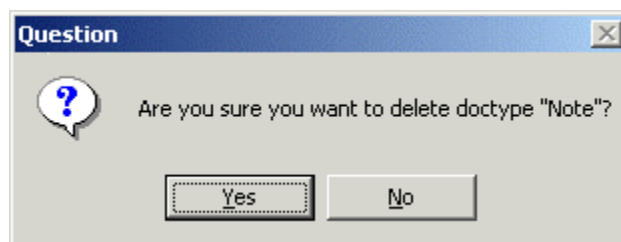


Figure 104: Confirming document type deletion

2. To delete the type, click **Yes**.

Associating Document Templates

Document types can be associated with document templates created in the Template Management Utility. For information on creating templates, see *Exigen Workflow Administrator's Guide, Part III: Utilities*, Chapter 8: Template Management Utility.

Each document type can have several associated templates. Each template can be associated with only one document type.

To associate document types with templates, proceed as follows:

1. In the **Project Document Types Setup** window, click **Templates**.

The **Associated Document Templates** window appears.

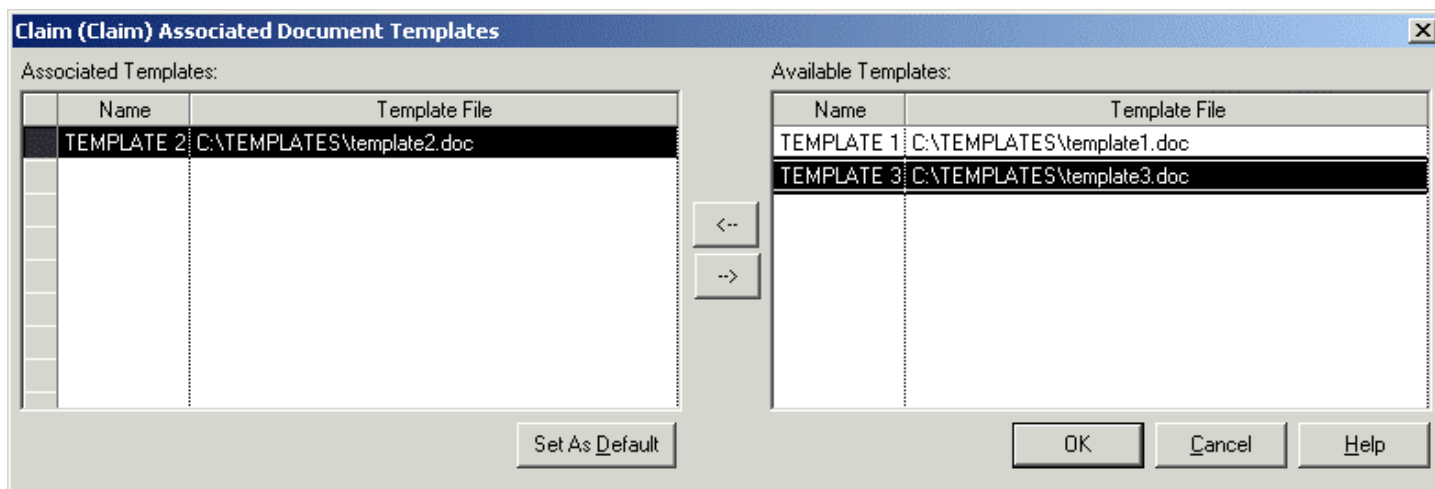




Figure 105: Assigning document templates

The **Associated Templates** list displays all document templates associated with the selected document type. The **Available Templates** list displays all available document templates defined in the selected project.

2. To assign a document template to the document type, in the **Available Templates** list, select the template and click .
3. To remove an assigned document template, in the **Associated Templates** list, select it and click .
4. To set one of the assigned document templates as the default, in the **Associated Templates** list, select a template and click **Set As Default**.
5. To apply changes, click **OK**.
6. To exit the window without saving changes, click **Cancel**.

Setting Up Skills

A **skill** defines a set of rules that allows managers to evaluate if this skill is required to process a specific parcel. Skill rule definitions are based on parcels and they are different for each project.

Skill-based parcel retrieval helps to organize processes more effectively by sending parcels to the most suitable person.

All skills must be assigned to a particular skill group. For example, skills *English* and *Spanish* belong to a *Language* skill group. If the administrator wants a particular user to be able to process only those documents that are in Spanish, the user must be assigned the *Language* skill group and, in the *Language* skill group, the *Spanish* skill must be selected. Skill groups are defined as columns in the skill table.

To implement skills in a project, perform the following main configuration steps:

1. In Configuration Browser, define skill groups by specifying the skill table format as described in [Defining Skill Groups](#).
2. Define skills as described in [Defining Skills](#).
3. Assign skills to users as described in [Assigning Skills to Users](#).

Note: This feature is not available in standard Exigen Workflow client/server and Web applications. It is supported by programmable extensions only, and is available via application programming interfaces (APIs). For information on how to acquire this feature, contact Exigen Support Services.

Defining Skill Groups

To define skill groups, proceed as follows:

1. In Workflow Explorer, select **Administration Tools > Workflow Tools > Configuration Browser**.

The **Configuration Browser** window appears.

For information on Configuration Browser, see [Viewing and Modifying Configurations](#).

2. Click **Add Section** .

The **New Section** window appears.

3. In the **Name** list box, select **Skills table format**.
4. In the **Project ID** field, enter the ID of the project in which the skills must be defined.

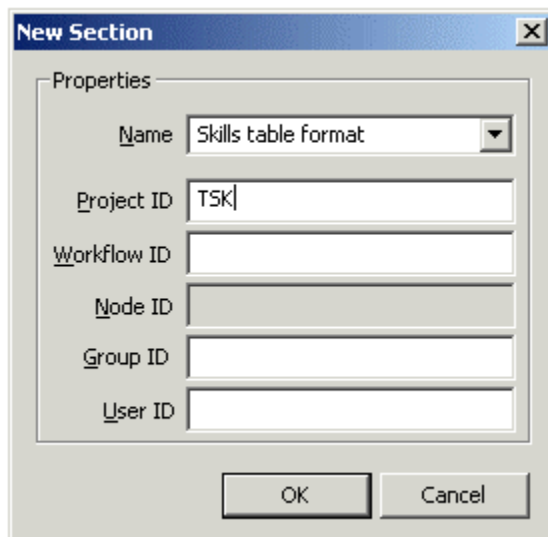


Figure 106: Defining a skill table format section

5. Click **OK**.
A new configuration section is created.
6. Configure the section as follows:
 - Set the **Column count** parameter value to the total number of skill groups.
 - For each skill group, create a **Column** section.
 - In each **Column** section, set the **ID** parameter value to a unique sequential number.
 - In each **Column** section, set the **Header** parameter value to a skill group name followed by the slash / symbol, for example *Language/*.

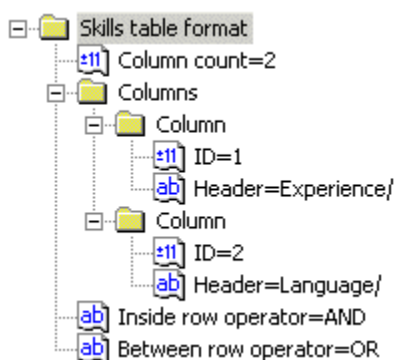


Figure 107: Skill table format example

7. Close Configuration Browser.

Defining Skills

To define skills, proceed as follows:

1. In Workflow Explorer, select **Administration Tools > Workflow Tools > Administrator**.

The **Administrator Utilities** window appears.

2. Click **System Setup** .

The **System Setup** window appears.

3. Click **Skills Setup** .

The **Skills Setup** window appears.

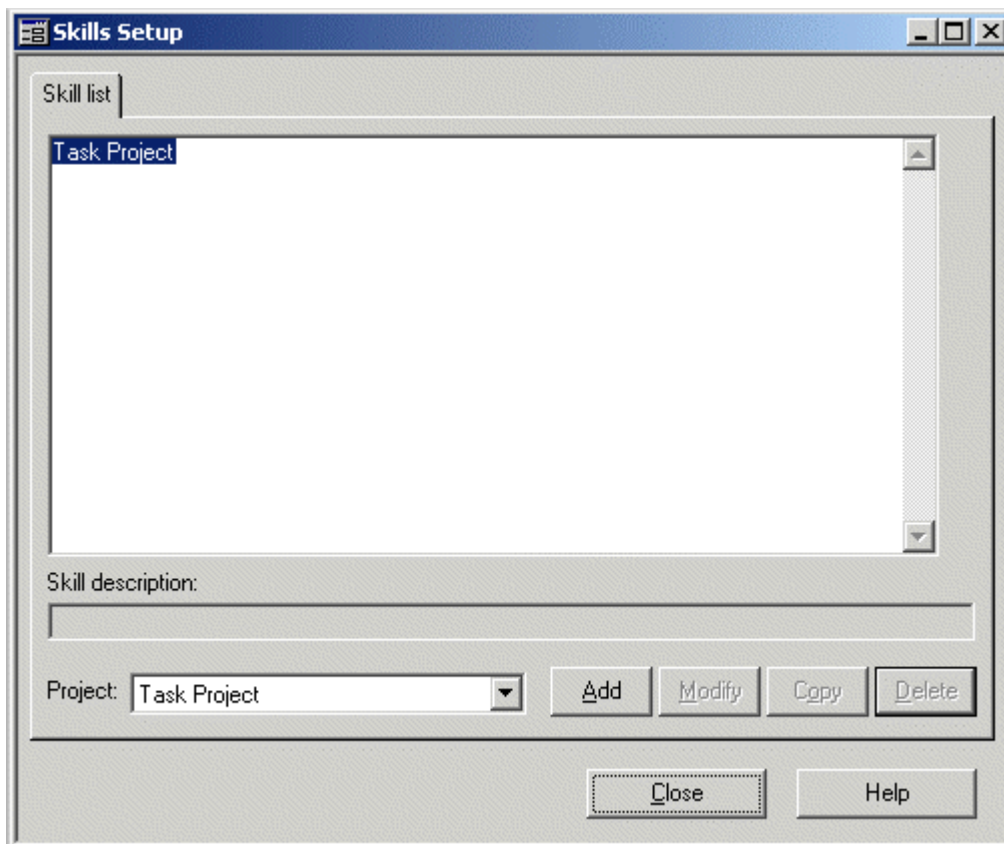


Figure 108: Skills Setup window

4. In the **Project** list box, select the required project.
5. To create a new skill, click **Add**.

The **Add skill** window appears.

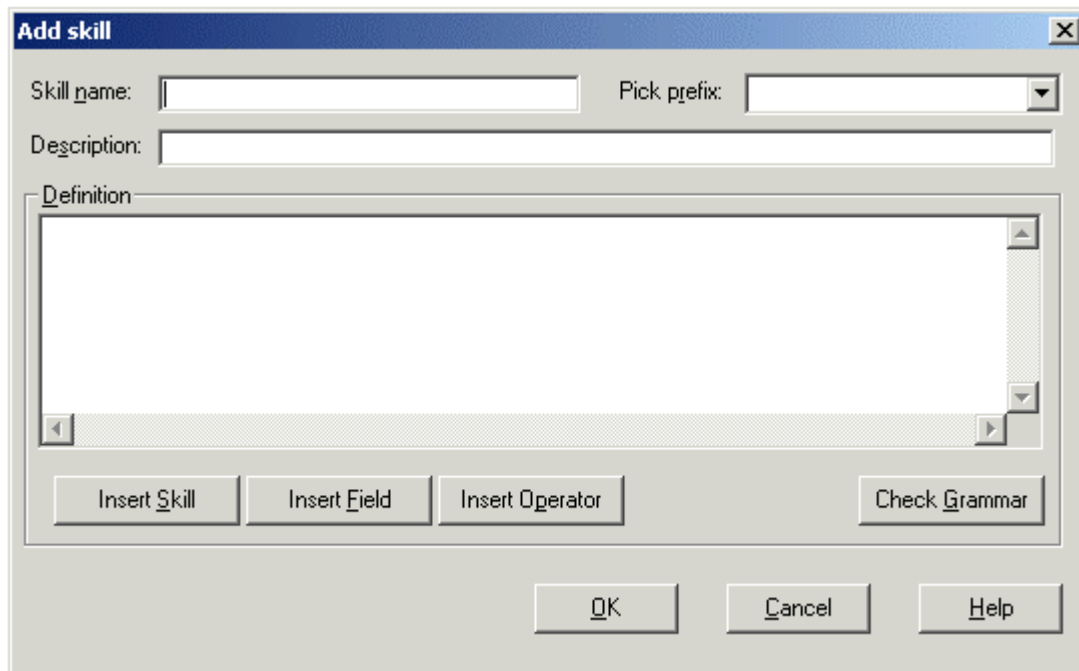
The image shows a Windows-style dialog box titled "Add skill". It has a blue title bar with a close button (X) in the top right corner. Inside the dialog, there are three input fields: "Skill name:" with a text box, "Pick prefix:" with a dropdown menu, and "Description:" with a text box. Below these is a large text area labeled "Definition" with a scroll bar. At the bottom of the dialog, there are four buttons: "Insert Skill", "Insert Field", "Insert Operator", and "Check Grammar". At the very bottom, there are three buttons: "OK", "Cancel", and "Help".

Figure 109: Adding a new skill

6. In the **Pick prefix** list box, select the skill group to which the new skill must be added.

The **Skill name** field is updated with the skill group name.

7. Supplement the **Skill name** field with the skill name so that the text in the **Skill name** field is in the following format:

```
<skill group>/<skill name>
```

The skill name can contain only alphanumeric characters and the underscore _ symbol.

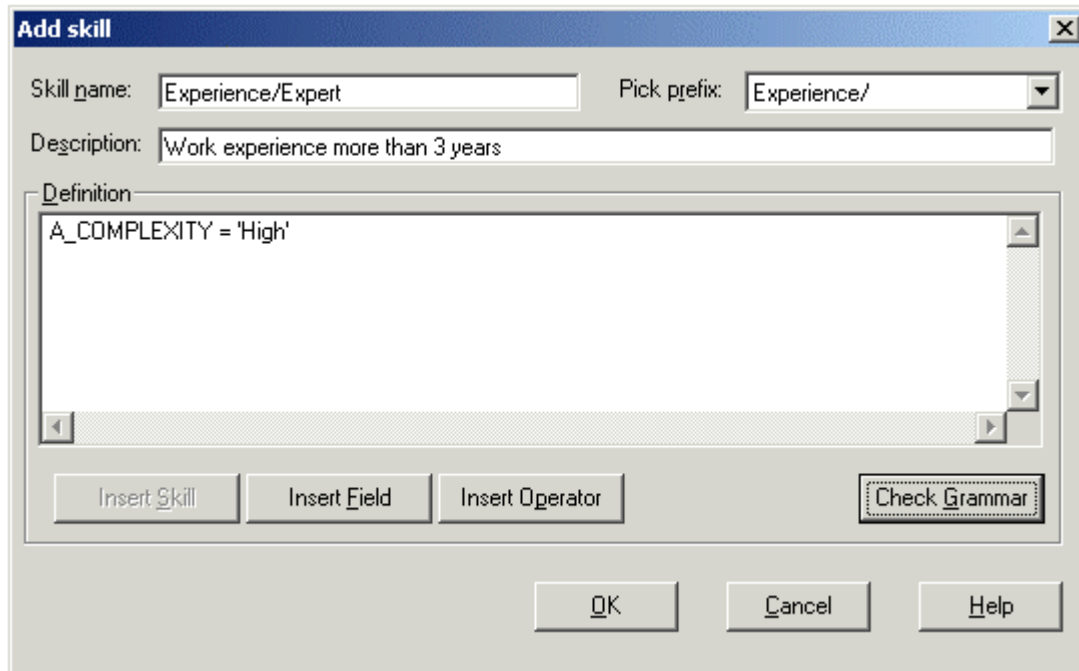
8. In the **Description** field, enter a standard WHERE statement that filters parcels matching this skill.

The statement can be entered manually or by using specific buttons as follows:

- To insert a table field, click **Insert Field** and select the required table field.
- To insert a logical statement operator, click **Insert Operator** and select the required operator.

9. To verify the correctness of the definition, click **Check Grammar**.

10. If any errors are displayed, correct them and click **Check Grammar** again.



The image shows a Windows-style dialog box titled "Add skill". It contains the following fields and controls:

- Skill name:** A text box containing "Experience/Expert".
- Pick prefix:** A dropdown menu showing "Experience/" with a downward arrow.
- Description:** A text box containing "Work experience more than 3 years".
- Definition:** A large text area containing the text "A_COMPLEXITY = 'High'".
- Buttons:** At the bottom, there are four buttons: "Insert Skill", "Insert Field", "Insert Operator", and "Check Grammar". Below these are three more buttons: "OK", "Cancel", and "Help".

Figure 110: Completed skill definition example

11. To save changes, click **OK**.

The new skills appear in the list.

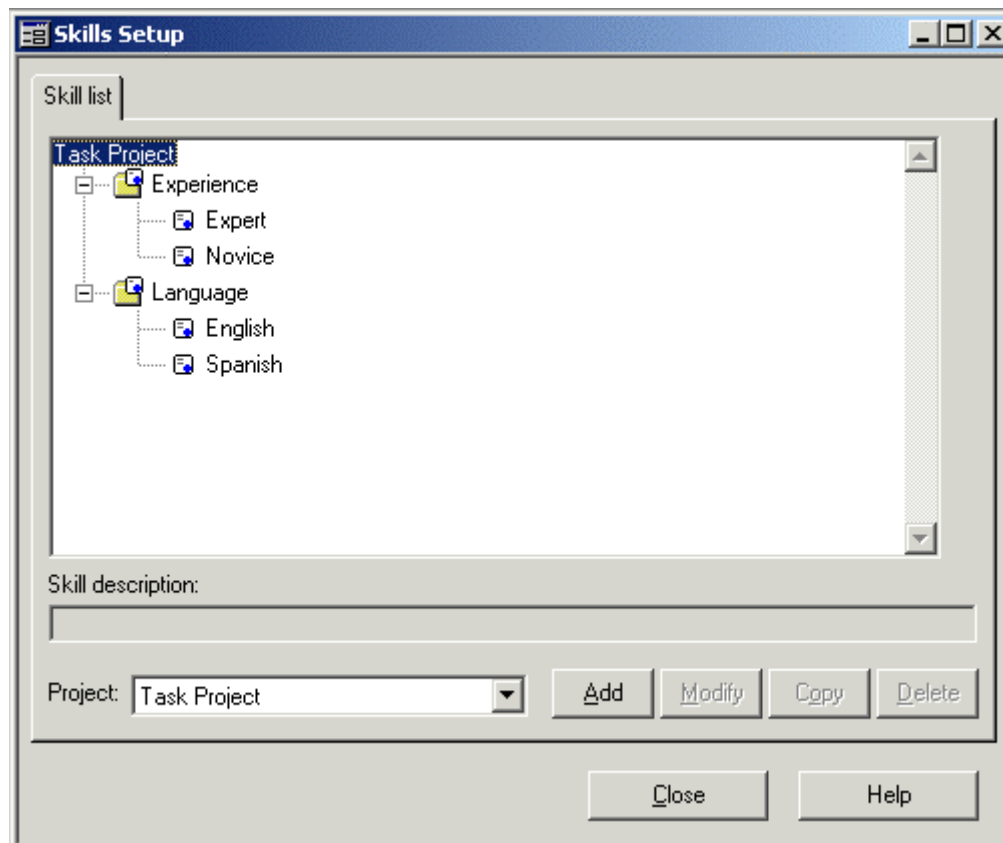


Figure 111: List of skills

12. To create a new skill based on the definition of another skill, select the source skill and click **Copy**.

The **Add skill** window appears for the new skill containing the definition of the source skill.

13. To delete a skill, select it and click **Delete**.
14. To modify a skill, select it and click **Modify**.
15. To close the **Add skill** window, click **Close**.

Assigning Skills to Users

Users must be associated with specific skills so that parcels are routed to users whose skills match parcel processing requirements.

To assign skills to a user, proceed as follows:

1. In Workflow Explorer, select **Administration Tools > Workflow Tools > Administrator**.

The **Administrator Utilities** window appears.

2. Click **Workflow User Setup** .

The **User Setup** window appears.

3. Select the **Skills** tab.

The image shows a 'User Setup' dialog box with four tabs: 'Users', 'Document Types', 'User in Groups', and 'Skills'. The 'Skills' tab is selected. Inside the dialog, there is a 'Project:' dropdown menu set to 'Task Project' and a 'User:' dropdown menu set to 'JOHNC'. Below these is a 'Skill Table' with two columns: 'Experience' and 'Language'. The table has 10 rows. To the left of each row is a small square checkbox. Below the table are six buttons: 'Add Row', 'Copy Row', 'Delete Row', 'Move Up', 'Move Down', and 'Definition Copy'. At the bottom of the dialog are three buttons: 'Apply', 'Close', and 'Help'.

	Experience	Language
<input type="checkbox"/>		
<input type="checkbox"/>		
<input type="checkbox"/>		
<input type="checkbox"/>		
<input type="checkbox"/>		
<input type="checkbox"/>		
<input type="checkbox"/>		
<input type="checkbox"/>		
<input type="checkbox"/>		
<input type="checkbox"/>		

Figure 112: Assigning skills to a user

4. In the **Project** list box, select the required project.
5. In the **User** list box, select the user to whom the skills must be assigned.
6. To add a new skill entry, click **Add Row**.

A new row is added to the skill table. Each field in the row represents a skill group.

7. In the new row, click each field to select the required skill.

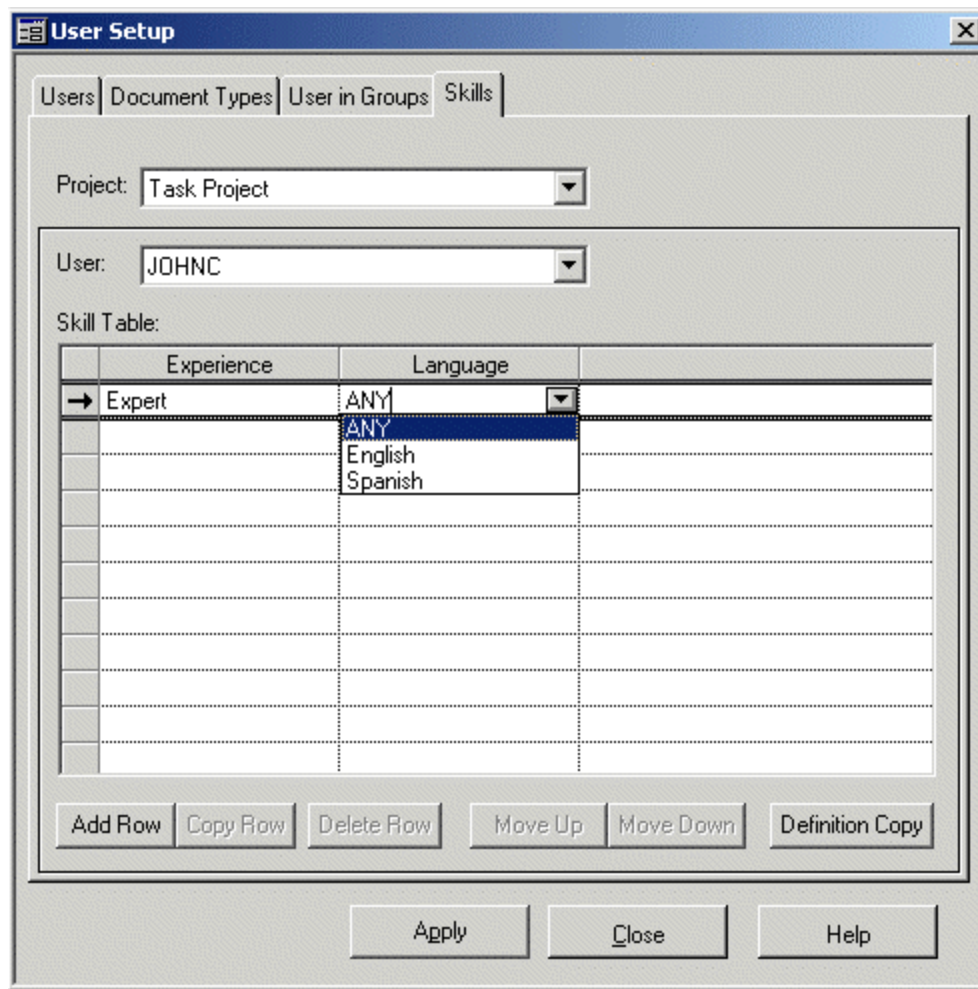


Figure 113: Selecting skills for each skill group

8. To move a skill up in the table, select it and click **Move Up**.
9. To move a skill down in the table, select it and click **Move Down**.
10. To copy a skill entry, select it and click **Copy Row**.
11. To copy the skill entries to another user, click **Definition Copy** and follow instructions as described in [Copying the Skill Definition](#).
12. To save changes, click **Apply**.
13. To close the window, click **Close**.

Copying the Skill Definition

To copy the whole set of skill entries to another user, proceed as follows:

1. In the **User Setup** window, in the **Skills** tab, click **Definition Copy**.

The **Definition Copy** window appears.

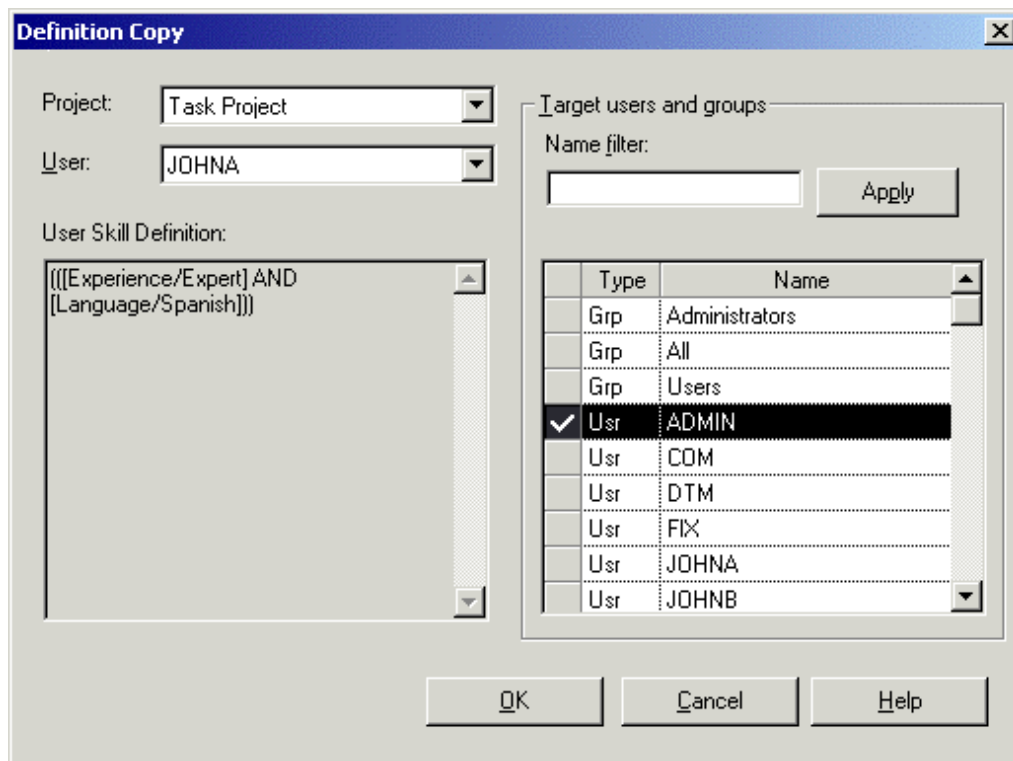


Figure 114: Copying the user's skill definition

The **User Skill Definition** text box displays the user's skill entries as a logical expression instead of a table. The table on the right displays all global groups and users defined in the system.

2. To find a specific user or group, in the **Name filter** field, enter the name and click **Apply**.
3. To select a group or a user to whom skill definitions must be copied, in the table, put a check mark next to the **Type** field.
4. To copy skill definitions, click **OK**.

Setting Up and Using Annotation Security

The following topics are included in this section:

- [General Procedure](#)
- [Example](#)

General Procedure

The following major steps are required for setting up and using annotation security:

1. If global user groups do not exist, define global user groups as described in [Setting Up Global User Groups](#).

This step is required because annotation security permissions are assigned to global user groups.

2. Define a document context security level for the particular annotation type as described in [Setting Up Document Context Security Levels](#).

For example, if the security level applies to posted notes annotations, the level can be named *Posted Notes*.

3. Retrieve a document and open it in the Image Viewer.

For information on working with the Image Viewer, see the *Exigen Workflow User's Guide*, Chapter 11: Image Viewer.

4. Create a secure annotation with a specified security level as described in the *Exigen Workflow User's Guide*, Setting Annotation Security in Chapter 11: Image Viewer.

Example

This example describes setting up and using annotation security for posted notes, which are electronic notes attached to Exigen Workflow documents.

In this example, two global user groups are created and are assigned different permissions for working with posted note annotations. An annotation is created and these permissions are tested.

One group, annotation administrators, is granted the following permissions for posted notes:

- view
- modify
- delete
- create
- change level

Another group, annotation managers, is granted the following permissions for posted notes:

- view
- modify

This section describes how to set up and use annotation security using the following procedures:

- [Creating a Security Level](#)
- [Adding a Secure Annotation to a Document](#)

Creating a Security Level

To create a security level, proceed as follows:

1. In the **Administrator Utilities** window, click **System Setup**.



2. In the **System Setup** window, click **Global User Groups Setup**.




3. In the **Global Users Groups** window, create two global user groups, AnnotAdmins and AnnotManagers, as described in [Adding a Global User Group](#).
4. To create a document context security level for posted notes, in the **System Setup** window, click



Document Context Security Levels Setup

The **Document Context Security Levels** window appears.

5. In the **Document Context Security Levels** window, click **Add**.
6. In the **Security Level ID** field, enter a security level, for example, *1*.
7. In the **Security Level Name** field, enter a security level name, for example, *Posted Note*.
8. To define permissions for posted notes, in the field on the right, select **Posted note**.
9. In the **User Groups** field, select **AnnotAdmins**.
10. To define annotation administrator permissions for posted notes, click the add/modify permissions button .

The **Assign/Modify permissions** window appears.

11. In the **Annotation Types** section, select **Posted note**.
12. To set annotation administrator permissions, in the **Permissions** section, select the following options:
 - **View**
 - **Modify**
 - **Delete**
 - **Create**
 - **Change level**

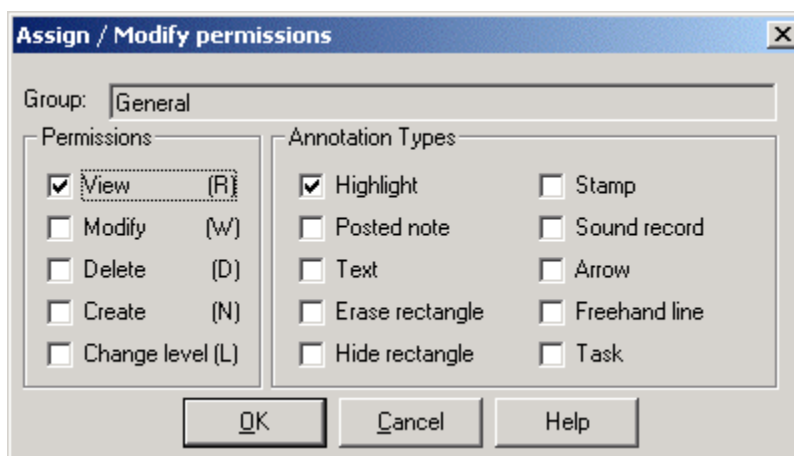



Figure 115: Assigning permissions for annotations

13. Click **OK**.
14. To set annotation manager permissions, in the **Document Context Security Level** window, in the right field, select **Posted note**.
15. In the **User Groups** field, select **AnnotManagers**.
16. Click the add/modify permissions button .
- The **Assign/Modify permissions** window appears.
17. In the **Annotation Types** section, select **Posted note**.
18. In the **Permissions** section, select the following options:
 - **View**
 - **Modify**
19. Click **OK**.
20. In the **Document Context Security Level** window, click **OK**.
21. In the **Document Context Security Levels** window, click **Close**.
22. To exit the **System Setup** window, click **Exit**.
23. To exit the **Administrator Utilities** window, click **Exit**.


Adding a Secure Annotation to a Document

To add a secure annotation to a document, proceed as follows:



1. To start Exigen Workflow, select **Start > Programs > Exigen Solution > Exigen Workflow > Workflow Explorer**.

The **Welcome to Exigen Workflow** window appears.

2. Log in as a member of the AnnotAdmins group.

3. In a node containing documents, select a document and click **Modify Image** .

The document is opened in the Image Viewer. For information on working with the Image Viewer, see the *Exigen Workflow User's Guide*, Chapter 11: Image Viewer.

4. To add a secure annotation, select the **Edit security** option.
5. Click the edit tools icon .
6. Click the electronic posted notes icon .
7. Position the cursor at the location in the document where the note is to be attached and double click.

The **Posted Notes** window appears.

8. To specify the text of the electronic note, in the top field, enter a text.
9. Click **OK**.

The **Security level assignment to object** window indicates whether the object is public or private and displays permissions. For more information on the **Security level assignment to object** window, see the *Exigen Workflow User's Guide*, Chapter 11: Image Viewer, Setting Annotation Security.

10. Select the posted notes security level and click **Assign to Selected Security Level**.
11. Click **OK**.

The electronic note is created as a secure annotation.

12. Exit the **Edit Tools** dialog and the Image Viewer.
13. Log on as a member of the AnnotManagers group.
14. Open the document with the electronic note.
15. View and modify the annotation.

If you attempt to perform other tasks, an error message appears indicating that the action is not allowed.

Maintaining Project Tables

Table Maintenance maintains all project tables. Some table records can only be added using this utility. For example, document types can only be added to the DOCTYPE table with this utility.

Note: Workflow Administrator **Table Maintenance** cannot be used to add records to workflow tables containing workflow-internal unique identifiers or RSNs, such as FOLDER, SUBFOLDER, BATCHPARCEL, DOCUMENT, EVENT, and DOCDETAILS. To add records to these tables, use workflow applications.

To maintain tables, proceed as follows:

1. In the **Administrator Utilities** window, click **Table Maintenance**.



Before opening the **Table Maintenance** window, Exigen Workflow asks whether you want to count the records.

2. If your database is quite large, click **No**, because the counting process can take a long time.

The **Table Maintenance** window appears.

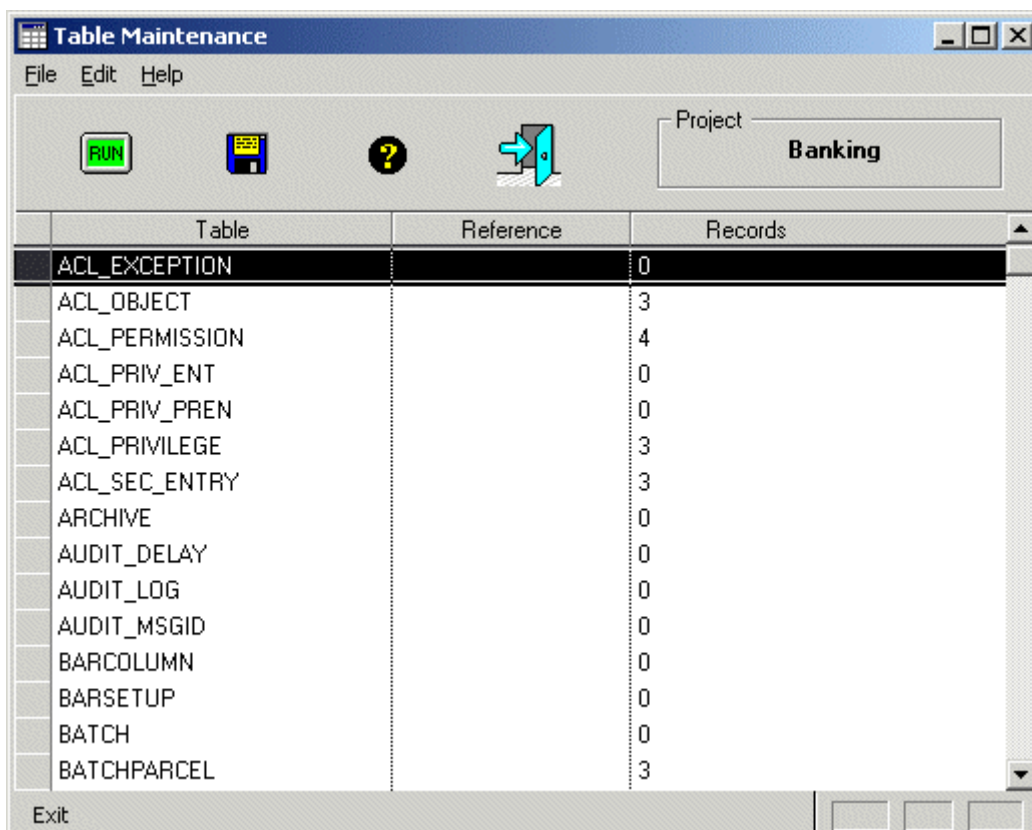


Figure 116: Table Maintenance window

The window lists all the tables in the selected project. A **Y** in the **Reference** column indicates the table values are also used as references for a field in another table. The **Records** column displays the number of records in the table.

- To view table records, select the table and click **Run**, or double click the table name.

A window appears, displaying available information on table records.

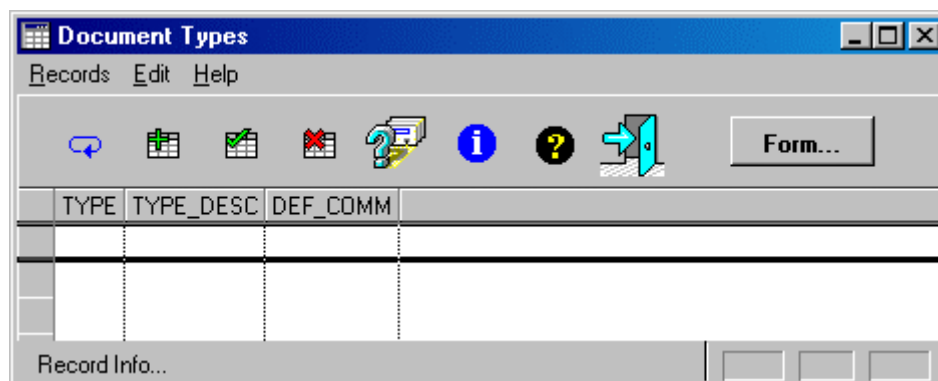


Figure 117: Displaying table records

If the record count in the selected table is greater than 25, the **Search for Table Records** dialog appears with the **Table** window.

4. To search for a table record, in the **Search for Table Records** dialog, enter search values.
5. To add a record, in the **Table** window, click **New Record**.



The **New Record** window appears.

	Field Description	Value
✓	Document Type	BILL
✓	Document Type Description	Bill
✓	Default days till commit	10

Figure 118: New Record window

6. Enter values for the table fields.
7. To return to the **Table records** window, click **OK**.
8. To modify a record, select the record and click **Modify**.
9. To delete a record, click **Delete**.
10. To see the current table record listing, click **Refresh**.
11. To open the **Search for Table Records** window, click **Query Table**.

The table lists search fields.

12. Enter the values for the records you are searching for and press **ENTER**.

All applicable records are listed in the window.

13. To see all table records again, click **Refresh**.

Maintaining Storage Locations

Storage Locations define where and how document images are stored after commit. This can be done in one of two ways:

- If you have a simple optical storage device, such as a jukebox, you can configure Exigen Workflow to optimally distribute files on this device. If this is the case, Exigen Workflow creates all required directories on the storage device and stores each committed file in one of these directories. When a directory reaches a certain size, files are stored to the next directory. If you use this system, you must select the **Optical** option as the **Commit type** in Project Configuration.
- If you use an optical device with special software installed, such as one that is capable of distributing files on its own, you can configure Exigen Workflow to pass the committed files to the server one by one. The server software is responsible for the files after that point. If you use this approach, you must select the **Server** option as the **Commit type** in Project Configuration.

You can set up both of these systems, especially if your company has a large number of locations worldwide. In this case, select the **Both** option as the **Commit type** in Project Configuration. When committing a file with this option enabled, a user can select the optical storage device or the server. Otherwise, only one of these options is available.

To manage storage locations, in the **Administrator Utilities** window, click **Optical Disk Utilities**.



If you configure your project to use both types of storage locations, Exigen Workflow asks whether you want to manage optical or server locations first. To configure optical devices first, click **Yes**.

The **Optical Disk Volume Maintenance** window appears.

Maintaining Optical Disk Devices

Optical Disk devices are the most commonly used option for document storage.

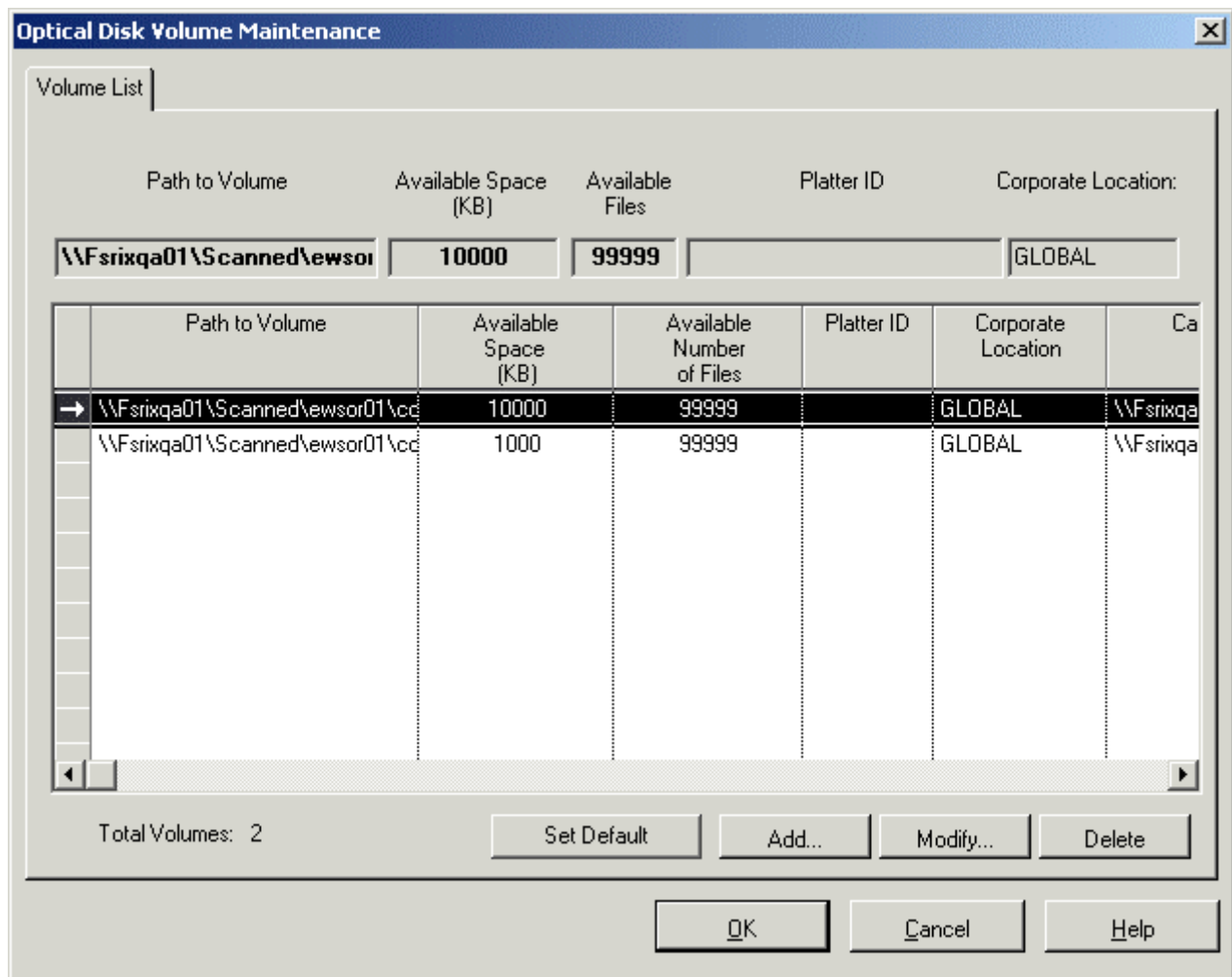


Figure 119: Optical Disk Volumes Maintenance window

Each entry in the **Volumes List** represents a directory on the optical device created by Exigen Workflow. One volume is considered one platter in the jukebox, and it can contain one or many directories.

To activate an optical disk configuration, select it and click **Set Default**.

To add a new optical disk device, volume, or directory, proceed as follows:

1. Click **Add**.

The **Add Configuration** window appears.

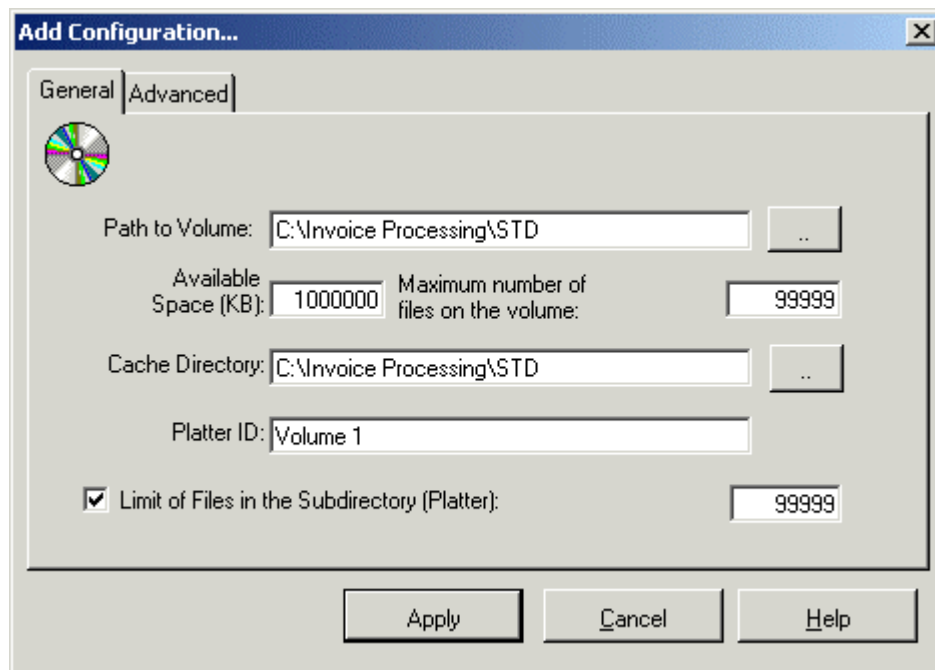


Figure 120: Add Configuration window, General tab

You can create one or more directories through this dialog. When selecting directory parameters, finding, copying, or moving a large directory with many files can take a long time.

2. In the **General** tab, select the appropriate options:

Add Configuration window, General tab	
Option	Description
Path to Volume	Path to the optical storage device entered by clicking the browse button. The three-letter project code is automatically added to the end of the path. When creating the actual directories, Exigen Workflow uses as a naming pattern the project code as the first three characters plus a five-digit index number such as 00001.
Available Space (KB)	Space allocated to the directory. If this limit is reached, Exigen Workflow does not store additional files in this directory. To restrict the directory by the number of files regardless of their total size, the largest amount possible must be entered in this field.
Maximum Number of Files on the Volume	Maximum number of files that can be stored in this directory. If this limit is reached, Exigen Workflow does not store additional files in this directory. Note that if you are creating several directories at the same time, this number reflects the total number of files in all directories. To restrict the directory by the total size of files regardless of their number, the largest amount possible must be entered in this field.
Cache Directory	Name for a directory that Exigen Workflow creates to temporarily store files retrieved from the optical device. This must be a network directory available to all users. If a file is modified after it is committed to optical storage, Exigen Workflow creates a new parcel for it and stores the file in the cache directory until it is recommitted.
Platter ID	Platter name. If a problem arises, its source can be easily tracked.

Add Configuration window, General tab	
Option	Description
Limit of Files in the subdirectory	Selected if you want to create several directories and restrict each one by the number of files in it. In the field that appears, the number of files in each directory must be entered. For example, if you want to create 50 directories with 100 files in each, enter 100 in this field and 5000 in the Maximum Number of Files on the Volume files.

3. Select the **Advanced** tab.

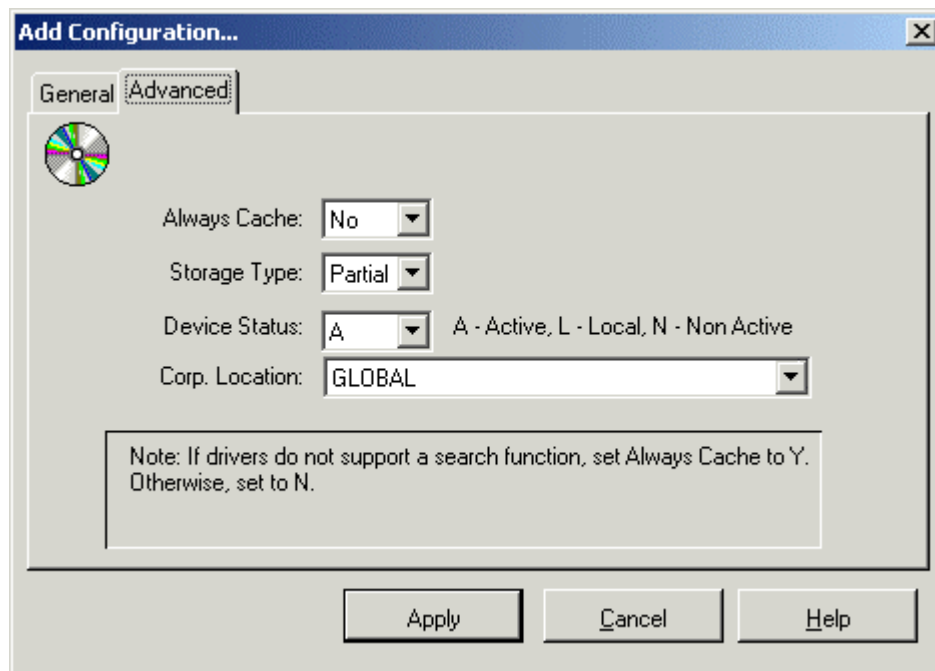


Figure 121: Add Configuration window, Advanced tab

4. In the **Advanced** tab, select the following options, if applicable:

Adding optical disk, Advanced tab	
Name	Description
Always Cache	System caches documents for read only, to free up more quickly optical devices that do not have their own cache functionality. Selecting Yes indicates files stored to the Cache Directory are specified in the General tab as soon as they are opened for viewing. Selecting No caches files only if they are modified.
Storage Type	Indicates how to store imaged document files in one of the following ways: <ul style="list-style-type: none"> • Full: stores all original imaged pages and image modification information together in one file. If a committed image is modified and recommitted, a new file with all the image information is created. This is recommended for small documents. • Partial: stores all imaged pages in one file and the image control information in another file. If a committed image is modified and recommitted, only the modification information is stored in a new file, with a reference to the location of the original file. This is recommended for large documents. • Single: stores each imaged page in one file and the image control information in another file.

Adding optical disk, Advanced tab	
Name	Description
Device Status	<p>Indicates one of the following status options:</p> <ul style="list-style-type: none"> A: Active if the device is functioning and available to all users. L: Local if the device is local to a user's computer and only that user has write access to the device, while others have read-only access. N: Non Active if the device is not currently being used or is not ready. <p>To perform operations successfully it is recommended that you select Active status.</p>
Corp. Location	Indicates corporate location of the device. This is helpful if you have several optical devices. If a storage problem arises, it is easier to track the source.

5. To add the new directory to the system, click **Apply**.

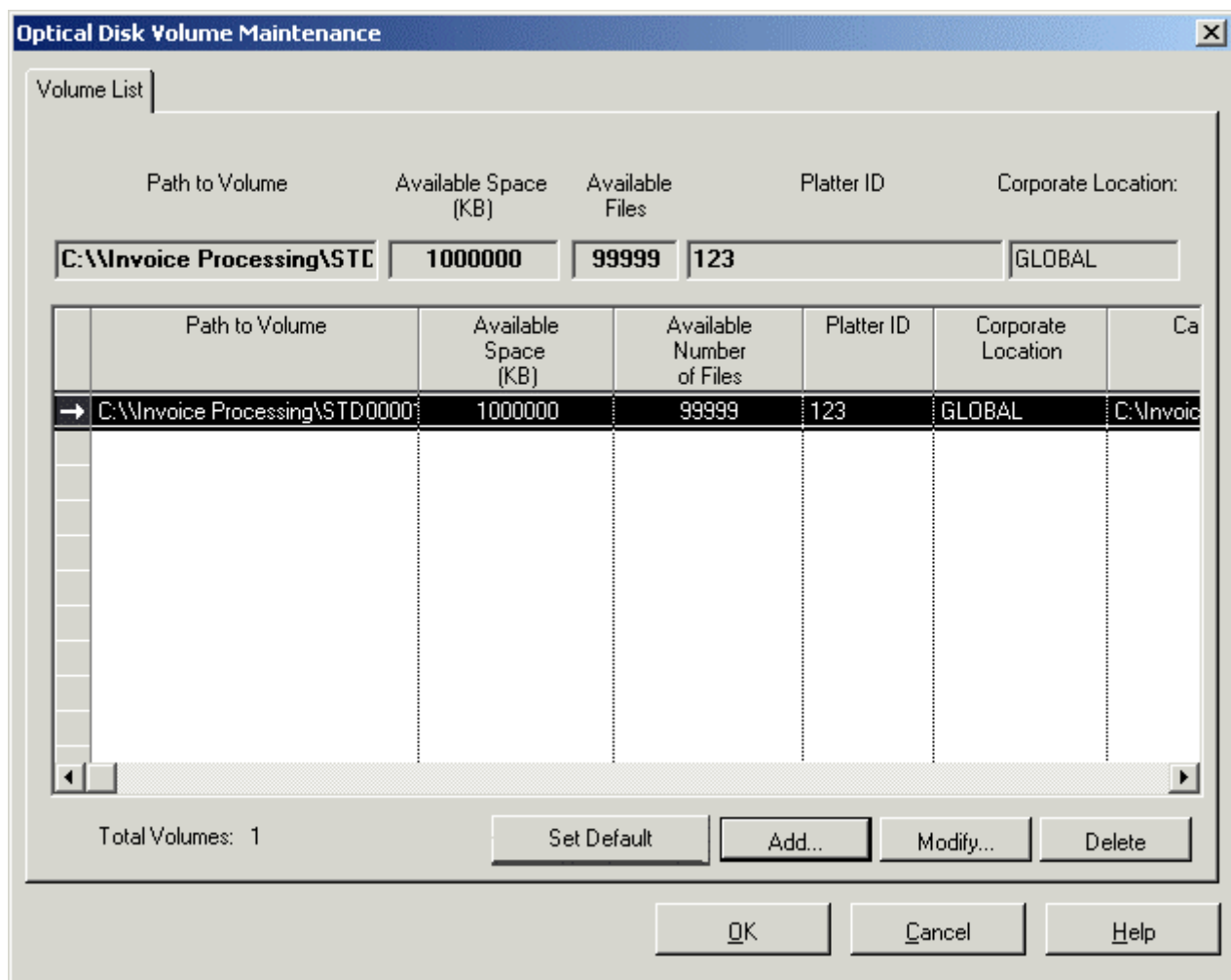


Figure 122: Optical Disk Volume Maintenance window

Exigen Workflow starts the commit process from the active directory and progresses down the list. The directories above the active one are ignored.

Ensure that you select the first active directory in the list before exiting this window.

To delete a directory configuration, select it and click **Delete**.

To modify a directory, proceed as follows:

1. Select the directory in the **Volumes List** and click **Modify**.

The **Modify Configuration** window appears.

2. In the **Modify Configuration** window, modify the directory settings.
3. Click **Apply**.

Maintaining Image Servers

Image Storage Servers are not used as often as **Optical Disk Volumes**, but are also supported by Exigen Workflow.

The **Image Server Setup** window that appears after closing the **Optical Disk Volumes** window is similar to the **Optical Disk Volumes** window.

To add a new image storage server, proceed as follows:

1. Click **Add**.

The **Add Configuration** window appears.

Add Configuration

General

Server type: [dropdown]

Host name: [text]

User name: [text] Password: [text]

DBM name: [text] Device status: A [dropdown]

Server cache: [text] ..

Cache directory: [text] ..

DMS directory: [text] ..

Corp. location: GLOBAL [dropdown]

Apply Cancel Help

Figure 123: Add Configuration window

The fields and options in the window differ depending on the selected server type.

2. In the **General** tab, enter the following values:

Adding Configuration window, General tab	
Field	Description
Server type	Image Server type. The following types are available: <ul style="list-style-type: none"> • Centera • FileNet • FileTech • IBM Content Manager
Host name	Server host name. For information on setting this parameter, see the server documentation.

Adding Configuration window, General tab	
Field	Description
Retention period	<p>Centera C-Clip retention period.</p> <p>This field appears only if Centera is selected as the server type.</p> <p>The following options are available:</p> <ul style="list-style-type: none"> • None: The C-Clip can be deleted at any time. • Infinite: The C-Clip can never be deleted. • Storage default: The retention period depends on the cluster setting. In the compliance plus model, the default retention period is infinite. In the basic compliance model, the default retention period is none. • User defined: The user defines the number of days in the retention period. The number is specified in the Days field.
Days	<p>Number of days in the Centera C-Clip retention period.</p> <p>If a number is specified in this field, the User defined option must be selected in the Retention period field.</p>
Separate pages	<p>If selected, DMS document pages are written to Centera in separate tags and can be retrieved individually.</p> <p>If cleared, the Centera solution stores DMS files without splitting them.</p>
User name and Password	Login information for the server's administrator.
DBM name	Database that the server uses. For information on setting this parameter, see the server documentation.
Device status	<p>Device status with the following options:</p> <ul style="list-style-type: none"> • A: Active if the device is functioning and available to all users • N: Not Active if the device is not in use
Server cache	Existing directory that the server uses to store its temporary files. For information on setting this parameter, see the server documentation.
Cache directory	Directory name that Exigen Workflow uses to temporarily store files retrieved from the image server. This must be a network directory available to all users. If a file is modified after it is committed to optical storage, Exigen Workflow creates a new parcel for the file and stores it in the cache directory until it is recommitted.
DMS directory	Directory name where DMS images are stored.
Corp. location	<p>Corporate location of the storage device.</p> <p>If corporate locations are not defined, the default, Global, is selected. If the Global option is selected, all users, independent of their corporate location, can use the device.</p> <p>If a corporate location is selected, only users from the specified corporate location can use the device.</p>

- To add the new server to the system, click **Apply**.

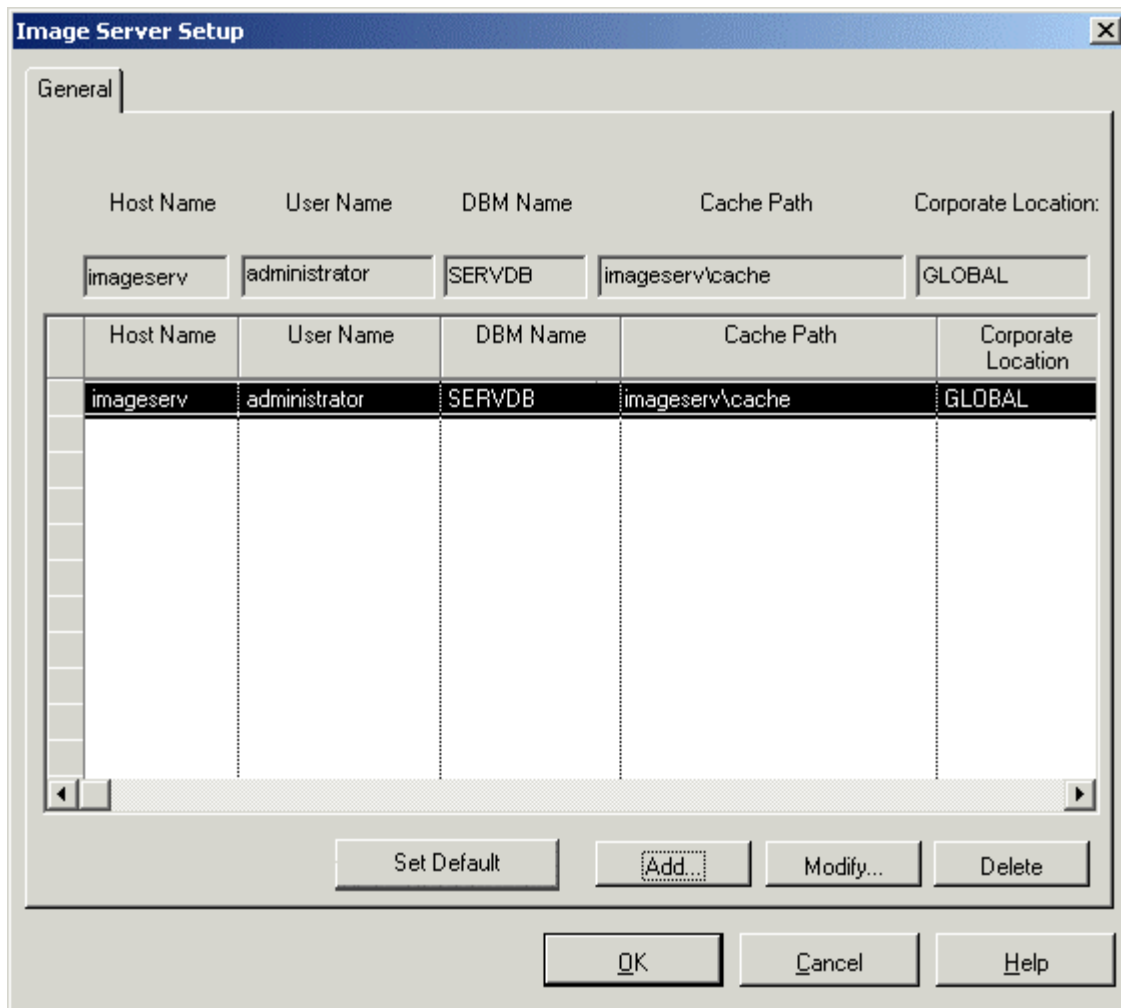


Figure 124: Image Server Setup window

To delete a server, select it and click **Delete**.

To activate a server, select it and click **Set Default**.

To modify a server, proceed as follows:

1. Select the server in the list and click **Modify**.

Exigen Workflow starts the commit process from the selected server and progresses down the list. The servers above the selected one are ignored.

2. Make sure that you select the first active server in the list before exiting this window.

Scheduling Activities

Activities Scheduler is a feature that allows the system administrator to schedule automatic activities for a project. An activity consists of a single event or a sequence of events.

Events are automatically performed jobs. The following two types of events are used in activities:

- Exigen Workflow predefined events, such as sending an email notification
- custom events for use with Advanced Event Server

The Activities Scheduler requires that an instance of Advanced Event Server is running on the workstation.

Note: In previous Exigen Workflow versions, Advanced Event Server processed events. Advanced Event Server is available in the `EventServer` folder of the Exigen Workflow installation CD and can be installed separately.

Advanced Event Server is replaced by Automatic Queue Server, and Automatic Queue Server handlers can be set up to process events. For more information on Exigen Workflow handlers, see the *Exigen Workflow Administrator's Guide, Part 2: Business Component Reference*, Chapter 21: Exigen Workflow Handlers.

Events are executed in the sequence in which they appear in the **Activity** window.

An activity can be scheduled once or at regular intervals. The following list provides examples of scheduled activities:

- Audit records are backed up automatically every 24 hours.
- Notes are removed from documents and all documents are printed at 8 a.m., December 1, 2004.

To use Activities Scheduler, the honor event date function must be enabled for the workstation where Advanced Event Server is installed. To enable the honor event date function, proceed as follows:

1. In the Windows Registry Editor, locate the `Honor Event Date` key in the following directory:

`HKEY_LOCAL_MACHINE\SOFTWARE\Datamax\Legacy Event Server\Parameters`

2. Set the `Honor Event Date` key value to 1.

To schedule an activity, proceed as follows:

3. In the **System Setup** window, click **Scheduled Activities Setup**.



The **Scheduled Activities** window appears.

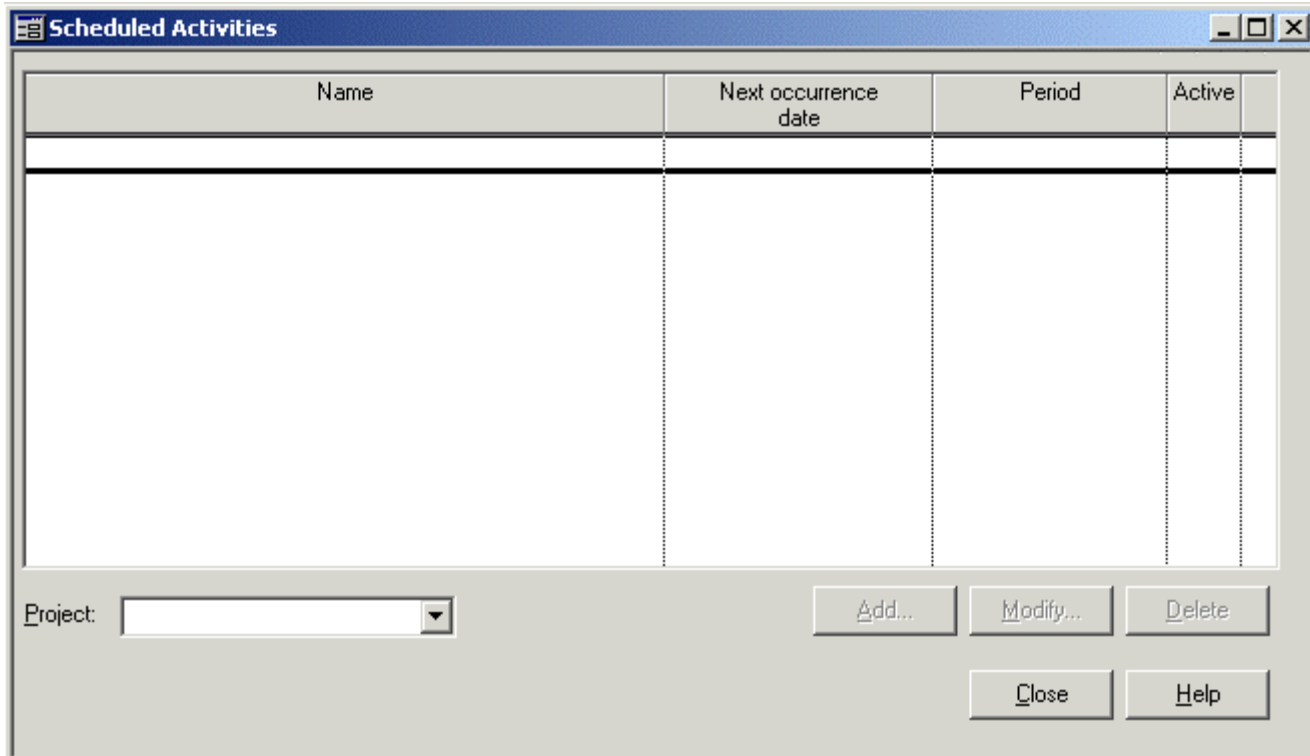


Figure 125: Adding a scheduled activity

4. In the **Project** field, click the arrow and select a project.
5. To add a scheduled activity, click **Add**.

The **Activity** window appears.

Activity

Name:

Next occurrence date:

Period:

☐ Active

Events

Event ID	Event name	Parameters

Figure 126: Defining a scheduled activity

6. In the **Name** field, enter a name for the activity.
7. To specify a date and time for the next activity occurrence, in the **Next occurrence date** field, edit the values.

For more information on setting a date and time, see [Activity Window](#).
8. To set an interval for repetition of the activity, in the **Period** field, enter the number of time units, for example, 3.
9. In the adjacent field, to specify the units of time, click the arrow and select **Seconds**, **Minutes**, or **Hours**.
10. To activate the activity, select the **Active** option.
11. To add an event, click **Add**.
12. To display a list of available events, in the **Event name** column, click at the right end of any field.
13. In the **Event ID** column, select an event name or enter an event ID.

The event ID appears automatically in the **Event ID** column.

14. If the **Edit** button is activated, to open a dialog for editing event parameters, click **Edit**.
15. If the **Edit** button is not activated, in the **Parameters** column, enter optional parameters manually.

For information on parameters and the **Edit** button, see [Activity Window](#).

16. To delete an event, select the event in the list and click **Delete**.
17. To add events, repeat steps 11 through 15 as required.
18. To change the sequence in which events are executed, select an event in the list and click **Up** or **Down**.
19. Click **OK**.

The new activity appears in the **Scheduled Activities** window, as described in [Scheduled Activities Window](#).

Scheduled Activities Window

The **Scheduled Activities** window is used to view, add, modify, and delete scheduled activities. The following table describes the **Scheduled Activities** window:

Scheduled Activities window	
Element	Description
Name	Activity name.
Next occurrence date	Date and time when the activity is next executed. The following examples show correctly entered dates and times: 12/02/2002 8:43:00 PM 12/02/2002 10:43:00 AM
Period	Interval between executions of the activity. For example, if the interval is 24 hours, the activity is executed daily.
Active	Indicates whether the activity is enabled. If an X appears, the activity is enabled.
Project	Project name in which the activity is executed. Selecting a project is mandatory.
Add	Opens the Activity dialog to add an activity.
Modify	Opens the Activity dialog to modify an activity.
Delete	Deletes the selected activity.
Close	Closes the window.
Help	Opens Help.

Activity Window

The **Activity** window is used to define a scheduled activity. The following table describes the **Activity** window:

Activity window	
Element	Description
Name	Activity name.
Next occurrence date	Date and time for the next execution of the activity. The following examples show correctly entered dates and times: 12/02/2002 8:43:00 PM 12/02/2002 10:43:00 AM

Activity window	
Element	Description
Period	Interval between executions of the activity.
Active	Indicates whether the activity is enabled. If an X appears, the activity is enabled.
Event ID	Event ID.
Event name	Event name.
Parameters	Optional parameters for the event. Event parameters differ depending on the event type.
Add	Adds an event.
Delete	Deletes the selected event.
Edit	Opens a dialog displaying event parameters. The button is enabled only if a dialog is available. If not, parameters are entered manually.
Up	Moves the selected event up the list. Events are executed in the order in which they are displayed.
Down	Moves the selected event down the list.
OK	Saves changes and closes the window.
Cancel	Closes the window without saving changes.
Help	Opens Help.

Audit Event Cleanup

Activities Scheduler is used to schedule cleanup of audit records at specified intervals.

Audit event cleanup requires that one or more archiving filters are set. For information on setting up archiving filters, see [Audit Archive Filter](#).

To schedule audit event cleanup, proceed as follows:

1. In Exigen Workflow Explorer, select **Workflow Tools**.
2. Double click **Administrator**.
3. In the **Administrator Utilities** window, in the **Project** list, select a project.
4. Select **Administrator > System Setup**.
5. In the **System Setup** window, select **Setup > Scheduled Activities**.
6. In the **Scheduled Activities** window, select an activity and click **Modify**.

The **Activity** window appears.

7. To open a list of events, in the **Activity** window, right click at the right end of the **Event name** column.
8. In the **Event name** list, select **Audit log housekeeping**.
9. Click **Edit**.

The **Audit Cleanup Event** window appears.

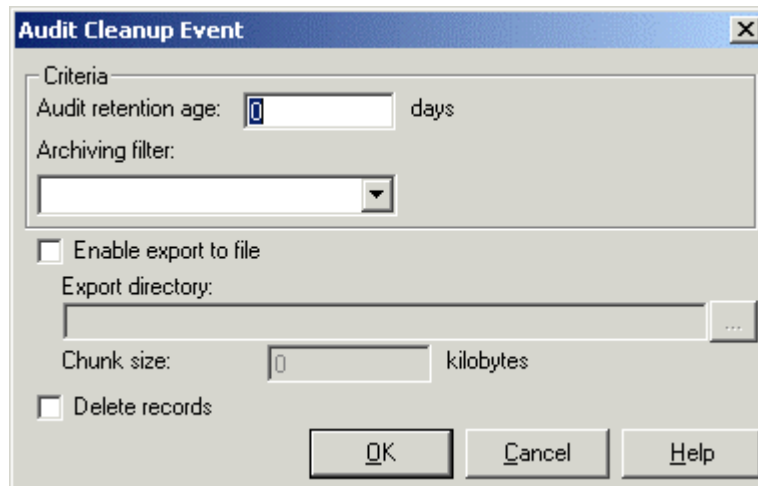


Figure 127: Specifying cleanup of audit events

10. To set the number of days that an audit record is retained before being exported or deleted, in the **Audit retention age** field, enter a value.
11. To specify the archiving filter, in the **Archiving filter** list, select a filter.
12. To enable audit record export to a file, select **Enable export to file**.
13. To specify the export directory for audit records, click the browse button next to the **Export directory** field.
14. To specify the maximum size of files to be exported, in the **Chunk size** field, enter a value.
15. To delete audit records after the specified retention period, select **Delete records**.
16. Click **OK**.

Audit records cleanup takes place at scheduled intervals.

Setting Up Document Access Control

For all projects using ACL based security, security settings must be specified in the **Document Access Control Setup** window.

The **Document Access Control Setup** window is used to specify privileges, entitlements, and permissions for documents, folders, and subfolders.

For information about privileges, entitlements, and permissions, see [ACL Based Security Concepts](#).

Setting up document access control consists of the following steps:

Defining document access control	
Step	Instructions location
1. Administrator defines users and global user groups.	See Setting Up Users . See Setting Up Global User Groups .

Defining document access control	
Step	Instructions location
2. Administrator defines privileges.	See Defining Privileges .
3. Administrator defines entitlements.	See Defining Entitlements .
4. Administrator defines permissions.	See Defining Permissions .
5. Administrator defines security entries.	See Defining Security Entries .
6. User specifies document security settings.	See the <i>Exigen Workflow User's Guide</i> , Chapter 4: High Volume Indexing, Specifying Document, Folder, and Subfolder Security Settings.

The following topics are included in this section:

- [Defining Privileges](#)
- [Defining Entitlements](#)
- [Defining Permissions](#)
- [Defining Security Entries](#)

Defining Privileges

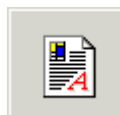
Privileges are defined by specifying a subset of system resources combined with a task that can be performed on them.

To define a privilege, proceed as follows:

1. In the **Administrator Utilities** window, click **System Setup**.



2. In the **System Setup** window, click **Document Access Control Setup**.



The **Document Access Control Setup** window appears.

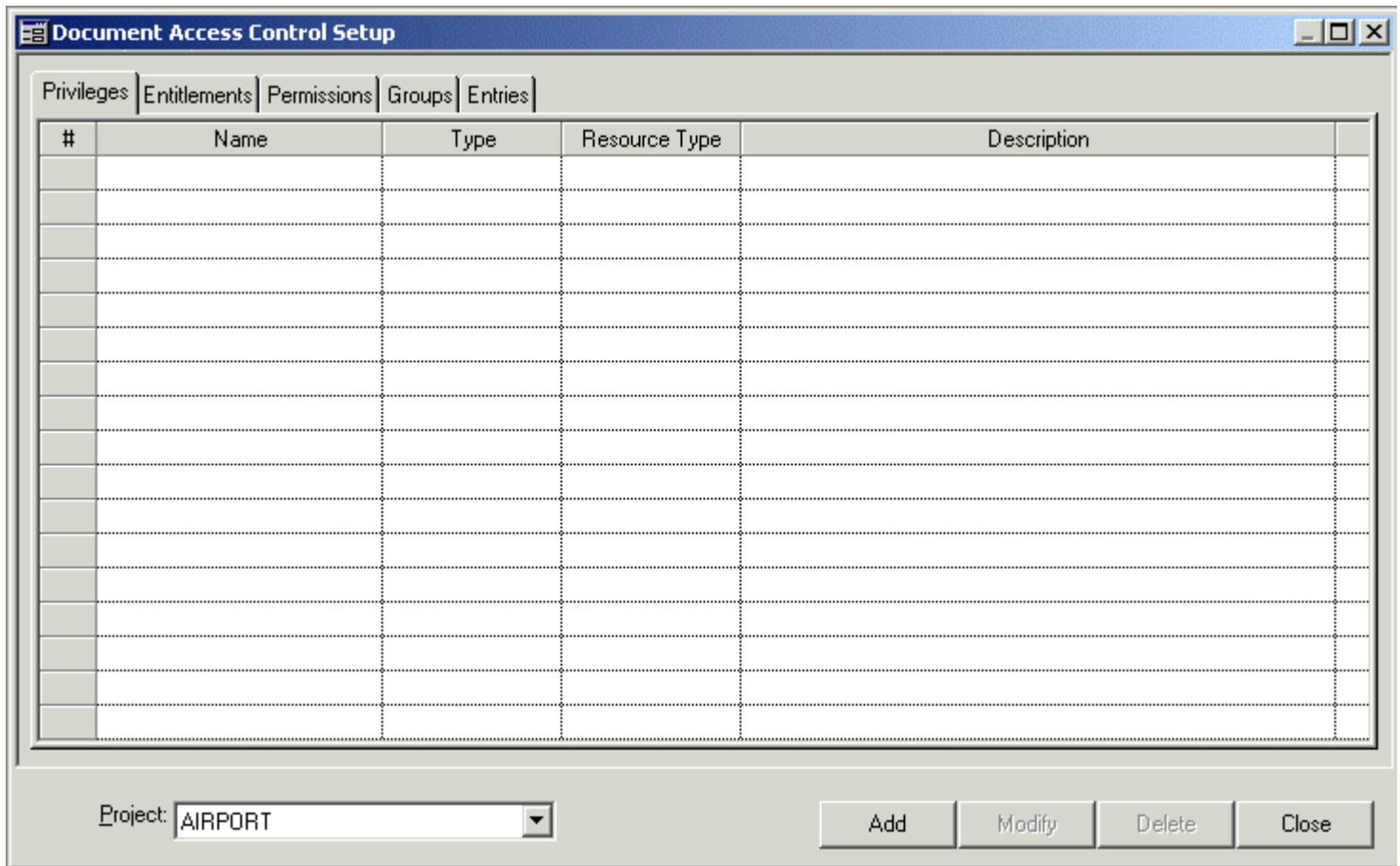


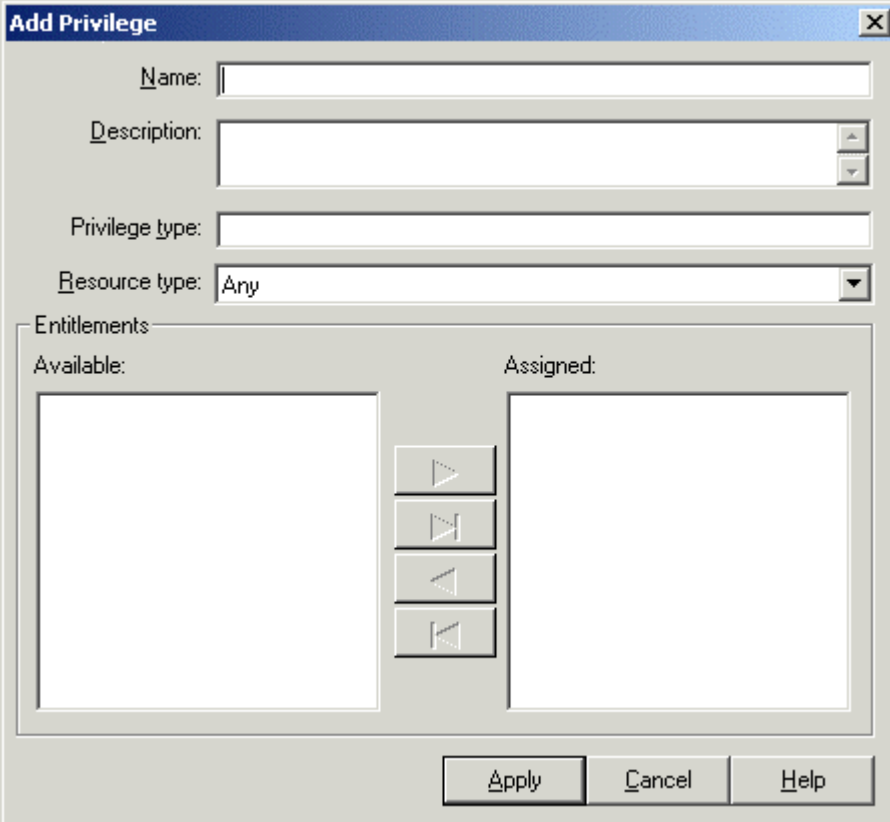
Figure 128: Specifying access control for documents, folders and subfolders

3. To define privileges, in the **Document Access Control Setup** window, ensure the **Privileges** tab is selected.
4. In the **Project** list box, select a project for assigning privileges.

Privileges can be assigned only for projects that have ACL based security activated. Only these projects are displayed in the **Project** list box. For more information on enabling ACL based security, see [Security Tab](#).

5. In the **Privileges** tab, to create a new privilege, click **Add**.

The **Add Privilege** window appears.



The 'Add Privilege' dialog box contains the following fields and controls:

- Name:** A text input field.
- Description:** A text input field with a vertical scrollbar.
- Privilege type:** A text input field.
- Resource type:** A dropdown menu currently showing 'Any'.
- Entitlements:** A section containing two lists:
 - Available:** An empty list box.
 - Assigned:** An empty list box.
 - Four arrow buttons (right, left, right, left) positioned between the two lists to move items.
- Buttons:** 'Apply', 'Cancel', and 'Help' buttons at the bottom right.

Figure 129: Specifying privileges

- To specify a name for a privilege, make an entry in the **Name** field.

An example of a privilege name is *Edit Medical Bills*.

- To describe the privilege, in the **Description** field, enter an optional description.

A privilege can be assigned a privilege type, which is an attribute. For example, if the privilege is *Edit Medical Bills*, the type can be *New York State*. In other words, the user can edit medical bills only for customers in the state of New York. The privilege type is optional and is assigned for the user's convenience.

- To specify the privilege type, in the **Privilege type** field, enter a type name.
- To specify the resource type to which the privilege applies, click the down arrow next to the **Resource type** field and select an option.

The following options are available:

Resource types	
Type	Description
Any	All resource types: documents, folders, and subfolders.
Document	Documents.
Folder	Folders.
Subfolder	Subfolders.

The **Entitlements** section contains a list of defined entitlements. Entitlements are assigned to privileges at a later stage in the process, as described in [Defining Entitlements](#).

10. To save changes and close the window, click **Apply**.

The privilege appears in the **Privileges** tab.

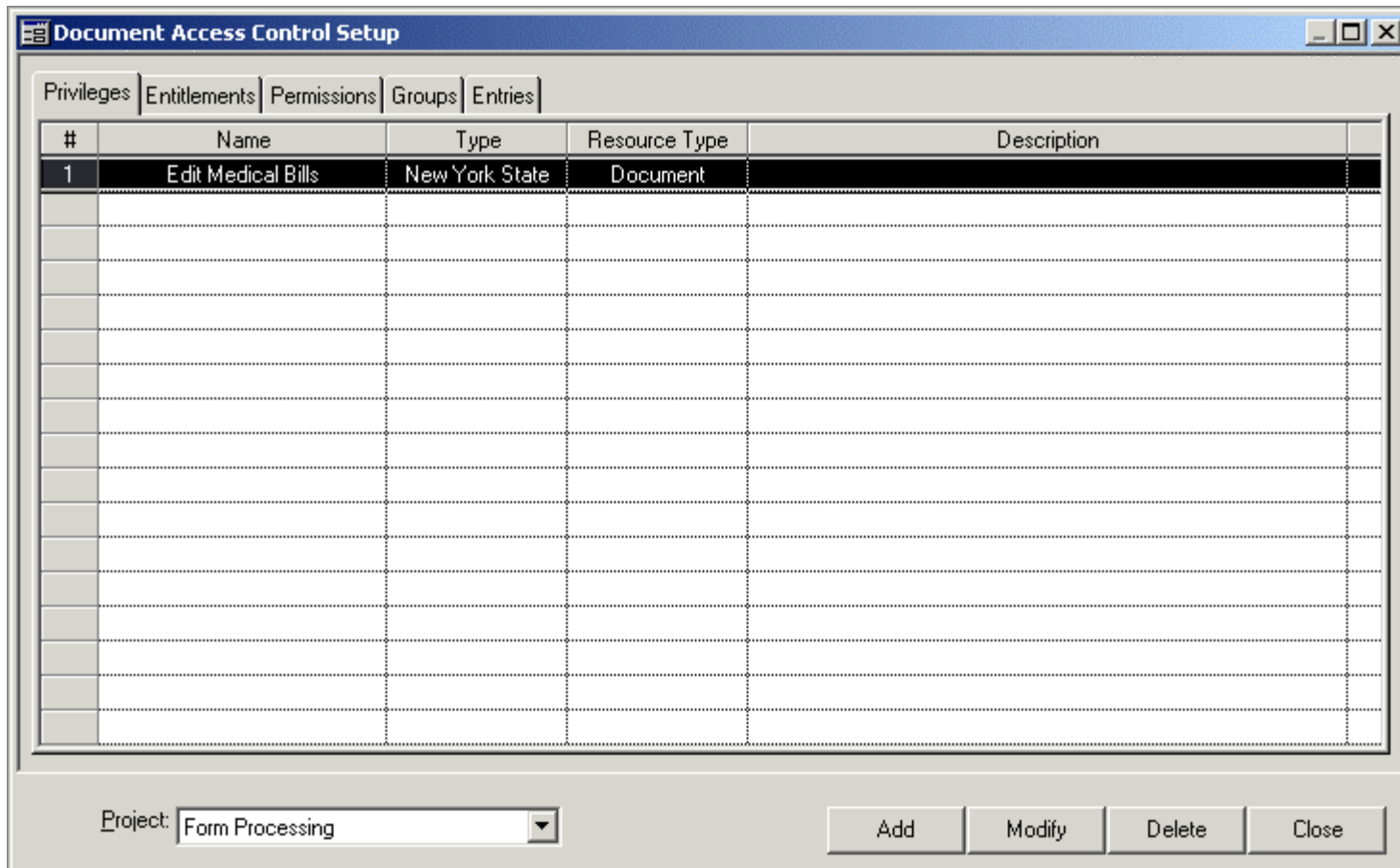


Figure 130: Viewing privileges

Defining Entitlements

Defining entitlements involves narrowing the scope of documents, subfolders, or folders to which security applies.

For example, to apply security only to the subset of documents that are medical bills, a document entitlement named Medical Bills is defined.

To define an entitlement, proceed as follows:

1. Select the **Entitlements** tab.
2. Click **Add**.

The **Add Entitlement** dialog appears.

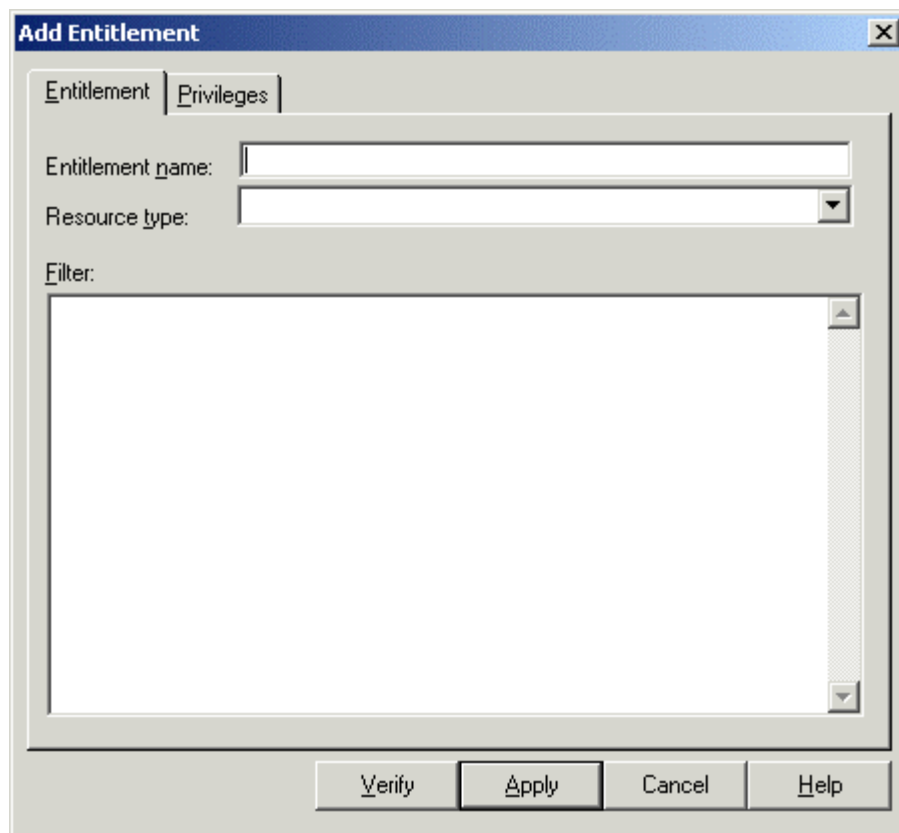


Figure 131: Defining an entitlement

- To specify an entitlement name, in the **Entitlement name** field, enter a value.

For example, enter *Medical Bills*.

- To specify the resource type to which the entitlement applies, in the **Resource type** field, select a resource type.

Selecting a resource type is mandatory. The following options are available:

Resource types	
Type	Description
Document	Applies to documents.
Folder	Applies to folders.
Subfolder	Applies to subfolders.

- To define the entitlement, in the **Filter** field, enter a valid SQL statement.

For example, to apply the entitlement only to documents of type Medical Bills, enter the following:

```
DOC_TYPE='A_MEDICAL_BILL'
```

- To verify the entitlement syntax, click **Verify**.

If the syntax is correct, a message indicates that the entitlement validation was successful.

If the syntax is incorrect, a message describes the error.

7. If required, in the **Filter** field, correct the syntax.
8. To assign the entitlement to privileges, select the **Privileges** tab.

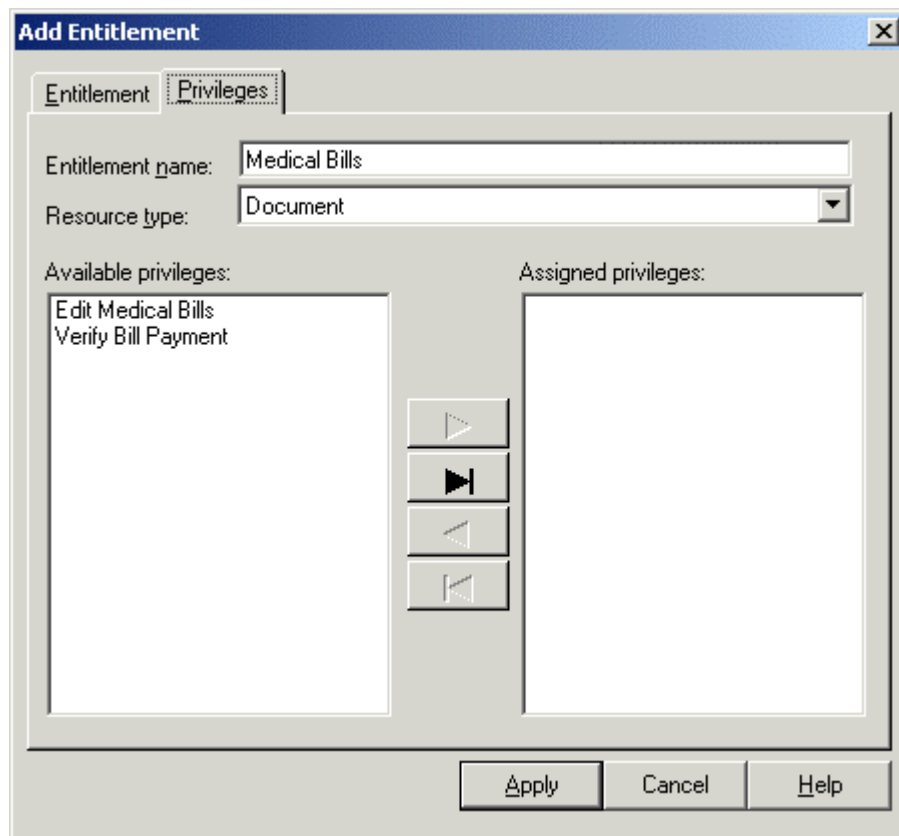






Figure 132: Adding an entitlement to a privilege

The **Available privileges** field displays all defined privileges having the same resource type as the entitlement. The **Assigned privileges** field displays privileges to which the entitlement is assigned.

9. To assign a privilege to the entitlement, in the **Available privileges** field, select the privilege and click **Add**  or double click the privilege.
10. To assign all privileges to the entitlement, click **Add all** .
11. To remove a privilege from the entitlement, in the **Assigned privileges** field, select the privilege and click **Remove**  or double click the privilege.
12. To remove all privileges from the entitlement, click **Remove all** .
13. To save the changes, click **Apply**.
14. To ensure that the entitlement is linked to the privilege, select the **Privileges** tab and double click the privilege.

In the **Modify Privilege** dialog, in the **Entitlements** section, the **Assigned** field displays assigned entitlements.

15. To close the **Modify Privilege** dialog, click **Cancel**.

Defining Permissions

Defining permissions involves specifying a set of tasks that can be performed with resources.

The following two examples illustrate the use of permissions:

- To ensure that administrators have complete access rights to all documents, folders, and subfolders, Full Access permission is defined. It includes the right to read, modify, delete, view, edit, and hide documents. Full Access permission is assigned to administrators by creating a security entry.
- To ensure that QA team members can only view, but not alter documents and images, Review permission is defined. Review includes the right to read and view documents. Review permission is assigned to QA team members by creating a security entry.

To define a permission, proceed as follows:

1. In the **Document Access Control** window, select the **Permissions** tab.

[illegible]

Figure 133: Defining permissions

2. To add a permission, click **Add**.

The **Add Permission** dialog appears.

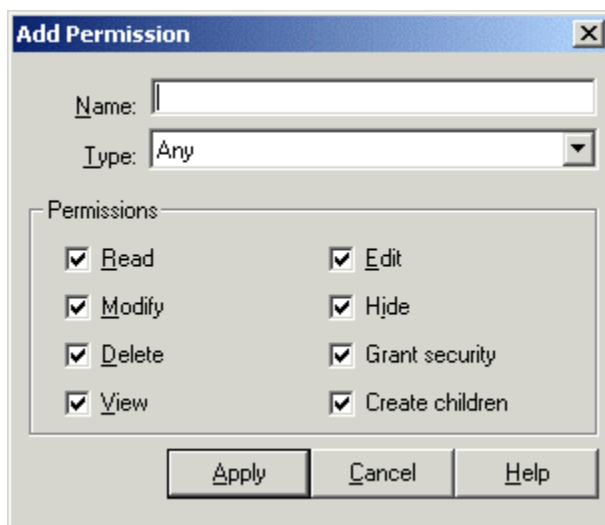


Figure 134: Adding a permission

3. To define a permission name, in the **Name** field, enter a value.
For example, a permission that provides rights to review documents is named *Review*.
4. To define a permission type, in the **Type** field, select the resources to which the permission applies.

The following options are available:

- **Any**
- **Document**
- **Folder**
- **Subfolder**

5. To define the operations allowed by the permission, in the **Permissions** section, select and clear the required operations.

The following operations are available:

- **Read**
- **Modify**
- **Delete**
- **View**
- **Edit**
- **Hide**
- **Grant security**
- **Create children**

For information on the operations, see [ACL Based Security Concepts](#).

6. To save the changes and close the window, click **Apply**.

The permission appears in the **Permissions** tab.

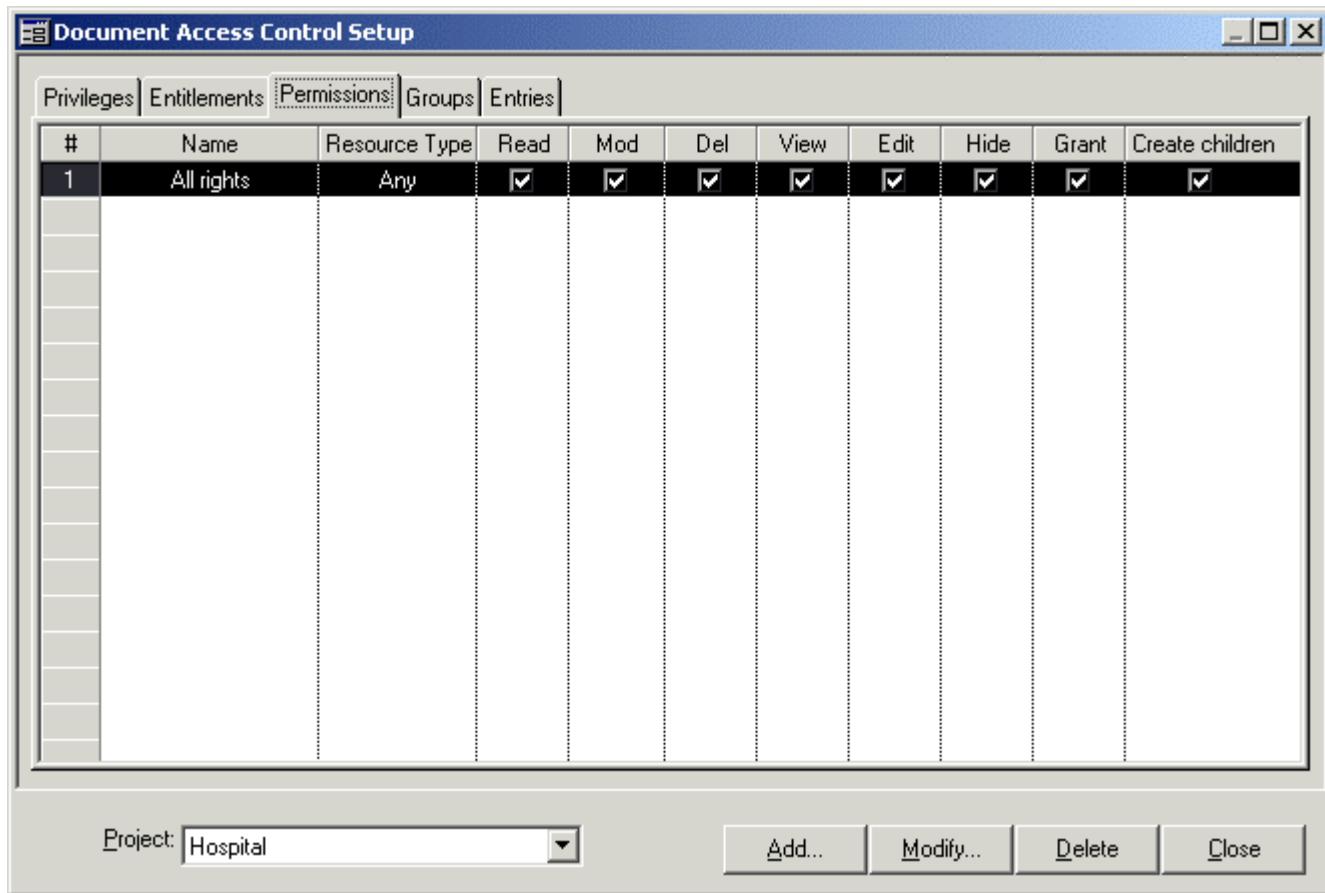


Figure 135: Viewing permissions

Defining Security Entries

Defining security entries involves combining privileges and permissions.

To define security entries, proceed as follows:

1. In the **Document Access Control Setup** window, select the **Entries** tab.
2. To add an entry, click **Add**.

The **Add ACL Entry** dialog appears.

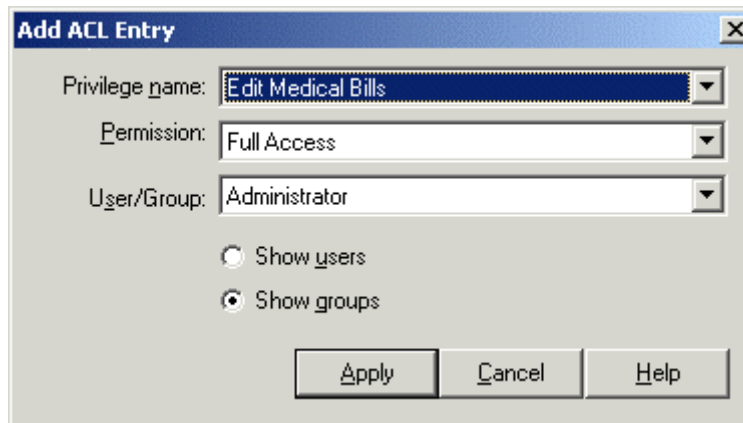


Figure 136: Adding a security entry

3. In the **Privilege name** field, select the privilege to be applied.

For information on defining privileges, see [Defining Privileges](#).

4. In the **Permission** field, select the permission to be applied.

The **Permission** list box displays only the permissions that have the same resource type as the selected privilege or have the *Any* resource type. If the selected privilege has the *Any* resource type, all permissions are displayed.

For information on defining permissions, see [Defining Permissions](#).

5. To select a user to whom the access rights apply, select the **Show users** option and, in the **User/Group** list, select the user.
6. To select a global user group to which the access rights apply, select the **Show groups** option and, in the **User/Group** list, select the user.
7. To apply the changes, click **Apply**.

The entry appears in the **Entries** tab.

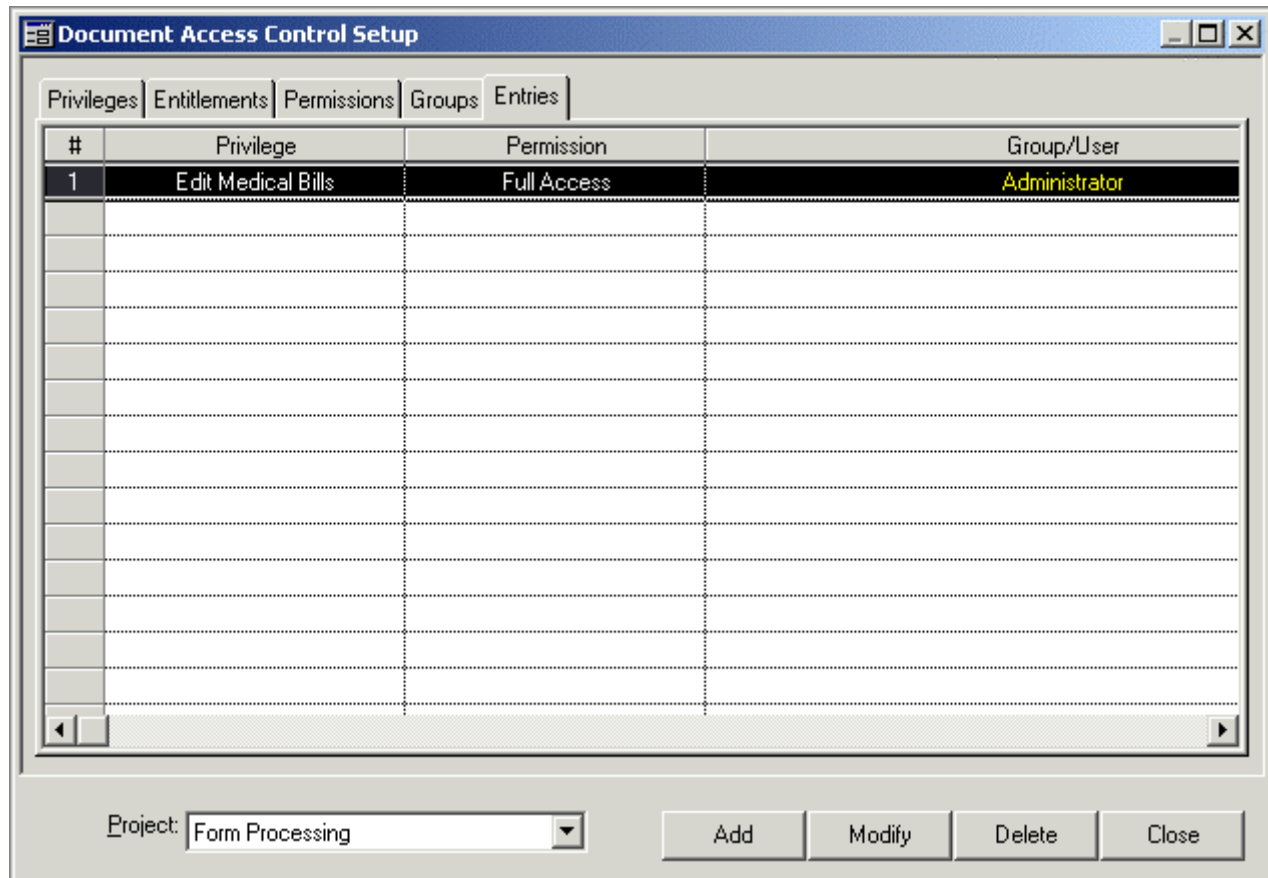


Figure 137: Viewing security entries

Setting Up and Printing Reports

To set up and print reports about the Exigen Workflow system, proceed as follows:

1. In Exigen Workflow Explorer, select the **Workflow Tools** folder and double click **Administrator**.
2. In the **Administrator Utilities** window, select **Administrator > System Setup**.
3. To set up the report, in the **System Setup** window, select **Setup > Reports**.

The **Setup Reports** window appears.

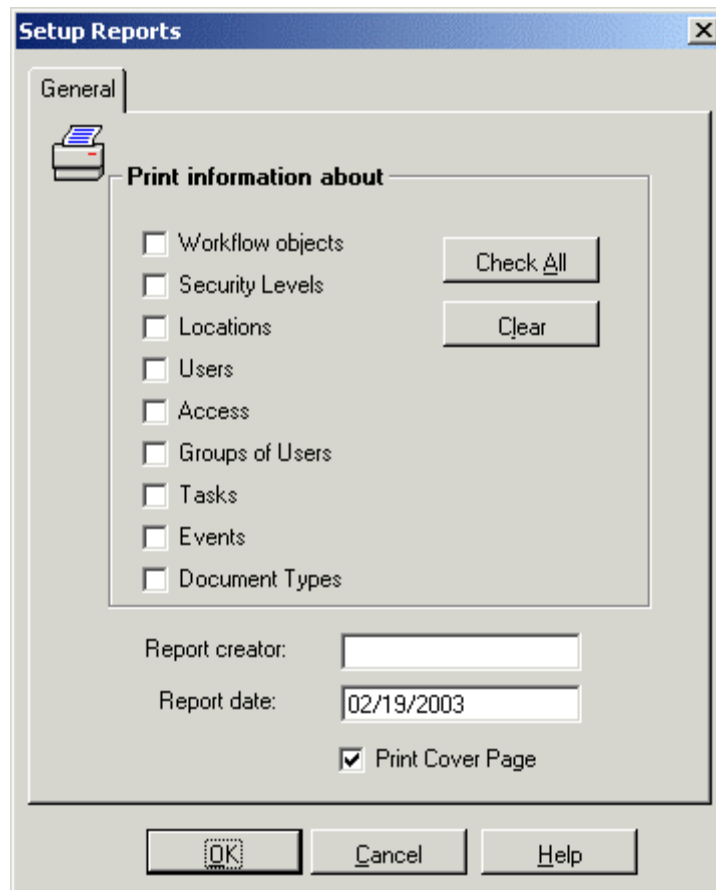


Figure 138: Setting up a report

4. To select the types of information to include in the report, in the **Print information about** section, select one or more of the following options:

Report information types	
Name	Description
Workflow objects	Exigen Workflow objects such as Retrieve, High Volume Scan, and Audit Server as described in Setting Up Workflow Objects .
Security levels	Security levels as described in Specifying Security Levels .
Locations	Corporate locations as described in Setting Up Corporate Locations .
Users	Exigen Workflow users as described in Setting Up Users .
Access	Access levels as described in Specifying Access Levels .
Groups of Users	User groups as described in Setting Up Workflow Groups .
Tasks	Task objects as described in Setting Up Tasks .
Events	Events as described in Setting Up Events .
Document Types	Document categories such as insurance claim or job application.

5. To select all report topics, click **Check All**.
6. To clear all selected report topics, click **Clear**.

7. To specify an author for the report, in the **Report creator** field, enter a name.

The **Report creator** field is optional.

8. To specify a date for the report, in the **Report date** field, enter a value.

The **Report date** field is optional. The default value is the current date.

9. To print a cover page for the report, select **Print Cover Page**.

The cover page contains the name of the report and the report author.

10. To cancel the print job, click **Cancel**.

11. To view a Help topic, click **Help**.

12. To view the report before printing, click **OK**.

The **CENTURA Report Builder** window displays the report text.

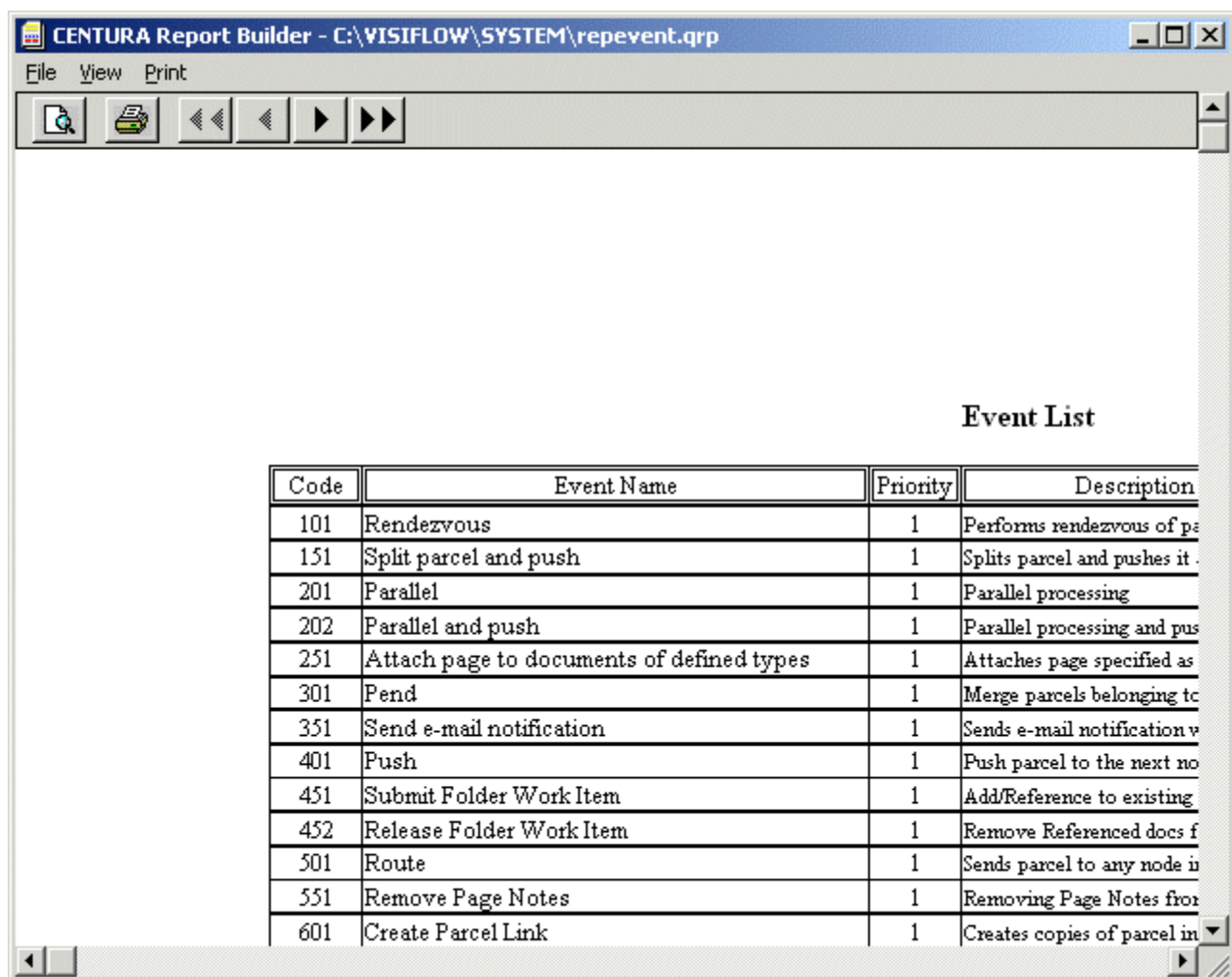








Figure 139: Viewing a report

13. To specify options for viewing the report, use the following buttons and menu commands:

Report viewing options		
Button	Menu command	Description
	File > Next Page	Scrolls to the next page.
	File > Last Page	Scrolls to the last page.
	File > Previous Page	Scrolls to the previous page.
	File > First Page	Scrolls to the first page.
	File > Go To Page	Scrolls to the selected page.
	File > Close Report	Closes the report.
	View > Actual Size	Displays the report at its actual size.
	View > Fit in Window	Modifies the report size to fit the window.

14. To specify printer settings for the report, select **Print > Printer Setup**.

15. To print the report, select **Print > Print** or click the print button .

The report is printed.

Viewing and Modifying Configurations

This section describes how to use Configuration Browser to view and modify Exigen Workflow configurations.

The following topics are included in this section:

- [What Is Configuration Browser?](#)
- [Configuration Browser User Interface](#)
- [Using Configuration Browser](#)
- [Managing Configuration Schemas](#)
- [Configuration Browser Menu Commands and Buttons](#)

What Is Configuration Browser?

Configuration Browser is an application used by system administrators to view and modify the configurations of Exigen Workflow components.

Configuration Browser is used to view and modify only the configuration settings stored in the S24_CONFIG table of the Exigen Workflow repository database. Configuration Browser specifies the configurations of Exigen Workflow servers, workflow nodes, and workflow tools.

Configuration Browser uses ODBC to access the Exigen Workflow database server. When started, Configuration Browser reads the existing configurations from the database server. When the existing configurations are updated, the updates are transferred back to the database server.

In all configuration sections, only modifications allowed by the Exigen Workflow schema can be made. The schema is a template for configuration data. The default schema is imported during the database update and cannot be changed by administrators.

Configuration Browser User Interface

The Configuration Browser user interface consists of a menu bar, two toolbars, and two main panes that display configuration settings.

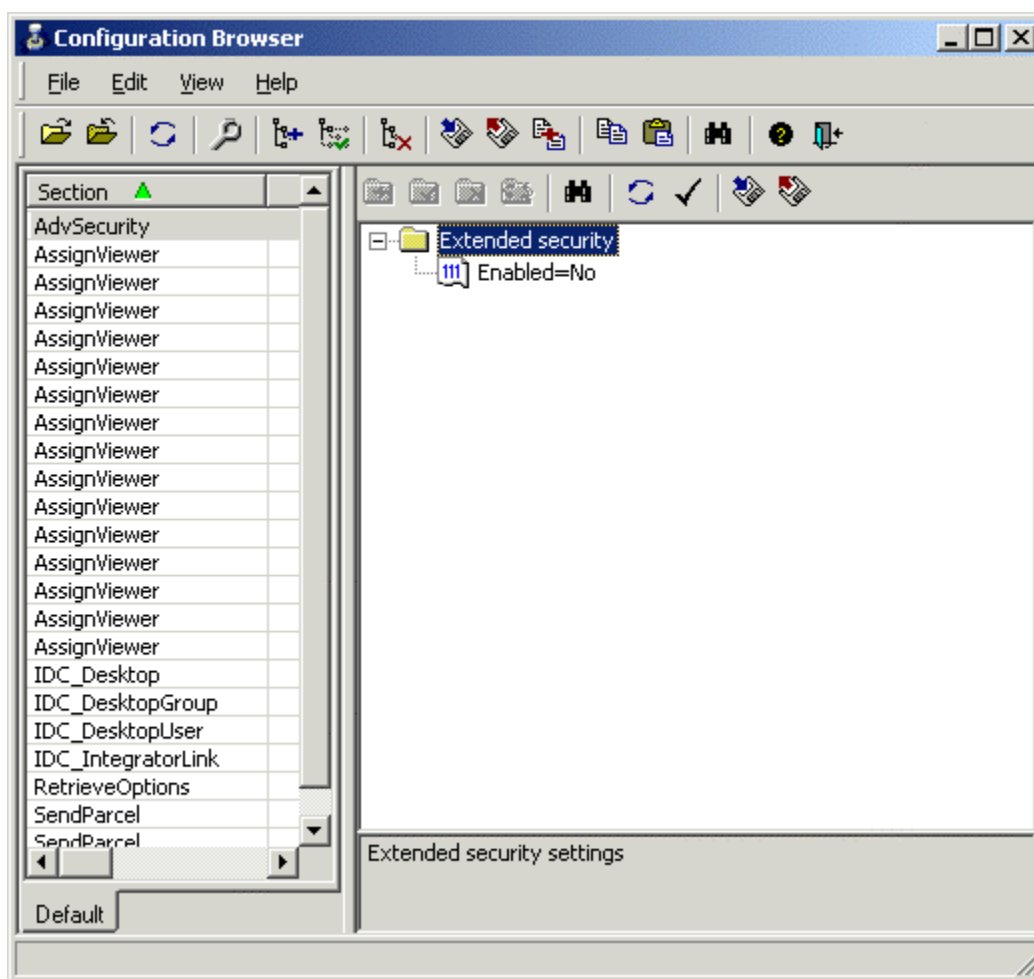


Figure 140: Configuration Browser

Menus are located at the top of the **Configuration Browser** window.



Figure 141: Configuration Browser menus

For information on menu commands, see [Menu Commands](#).

The left toolbar is located beneath the menus:



Figure 142: Left toolbar

For information on the left toolbar, see [Left Toolbar Buttons](#).

The right toolbar is located above the right pane.



Figure 143: Right toolbar

For information on the right toolbar, see [Right Toolbar Buttons](#).

The left pane contains a list of configurations.

Section ▲	UserId	NodeId	WfId	PrjId ▲
AUDIT_USER_FILTERS	DTM	0	0	
ActivityRegistrar				
AdvSecurity				
AssignViewer		2	47	
AssignViewer		3	44	
AssignViewer		3	45	
AssignViewer		5	44	
AssignViewer		5	45	
AssignViewer		6	47	
AssignViewer		7	47	
AssignViewer		8	45	
AssignViewer		11	47	
AssignViewer		12	47	
AssignViewer		13	47	
AssignViewer		14	47	
AssignViewer	BRUCE	1	25	
AssignViewer	BRUCE	2	25	
AssignViewer	DTM	1	1	
AssignViewer	DTM	1	2	
AssignViewer	DTM	1	3	
AssignViewer	DTM	1	5	
AssignViewer	DTM	1	6	
AssignViewer	DTM	1	7	
AssignViewer	DTM	1	8	
AssignViewer	DTM	1	9	

Figure 144: Configurations list

Each configuration has a name that is displayed in the **Section** column of the **Configuration Browser** window. Configurations that are user specific or dependent on the location in the workflow are defined by the following attributes:

- user ID
- node ID
- workflow ID
- group ID
- project ID

When a configuration section is selected, its nodes, items, and values appear in the right pane.

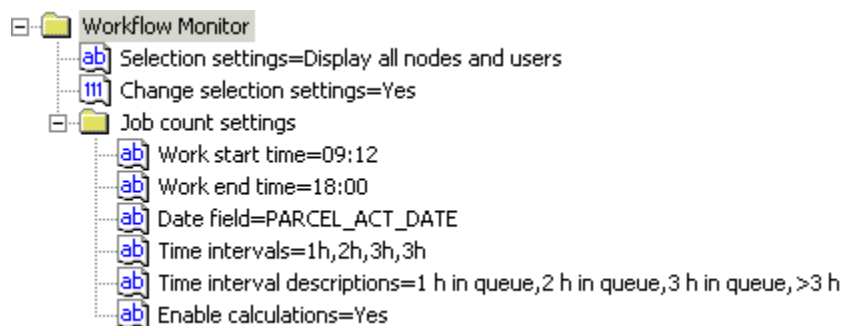


Figure 145: Configuration nodes and values

For example, a node is named **Job count settings**. An item within the node is named **Work start time**, and the value for **Work start time** is 09:12.

The icon to the left of the item name represents the value type. The following table describes value types:

Value types	
Icon	Type
	String. Can include letters, numbers, and symbols.
	Unsigned integer.
	Unknown value type. Cannot be edited.
	Float.
	Integer.
	Date and time.

Each configuration is a data tree consisting of nodes, subnodes, and values. The shape of the tree is specific to the component that uses the configuration. The administrator must know the supported node hierarchies and permitted values within the data tree. Only modifications that are allowed by the configuration schema can be performed. For information on configuration schemas, see [Managing Configuration Schemas](#).

Using Configuration Browser

The following topics are described in this section:

- [Starting Configuration Browser](#)
- [Specifying a Configuration View](#)
- [Opening a View](#)
- [Closing a View](#)
- [Switching Between Open Views](#)
- [Refreshing a View](#)
- [Adding a Configuration Section](#)
- [Editing a Configuration Section](#)
- [Deleting a Configuration Section](#)
- [Adding an Item](#)
- [Editing an Item](#)
- [Renaming an Item](#)
- [Undoing Unsaved Modifications](#)
- [Deleting an Item](#)
- [Copying and Pasting a Configuration Section](#)
- [Exporting a View](#)
- [Exporting a Configuration Section](#)
- [Importing a Configuration Section](#)
- [Exporting and Importing Configuration Data](#)
- [Exporting and Importing a Configuration Node](#)
- [Merging Configurations](#)
- [Setting User Preferences](#)
- [Searching for Items or Values in a Configuration Section](#)
- [Searching for Items or Values in Multiple Configuration Sections](#)
- [Sorting Items in the Configuration View](#)
- [Displaying and Hiding Columns in the Configuration View](#)
- [Exiting Configuration Browser](#)


Starting Configuration Browser

Before starting Configuration Browser, ensure that the **Configuration Browser** option is selected in Administration Utilities. A user can view and edit configuration settings only if the **Configuration Browser** option is selected.

For information on selecting the **Configuration Browser** option, see [Specifying Security Levels](#).

If Exigen Workflow is running, to start Configuration Browser, proceed as follows:

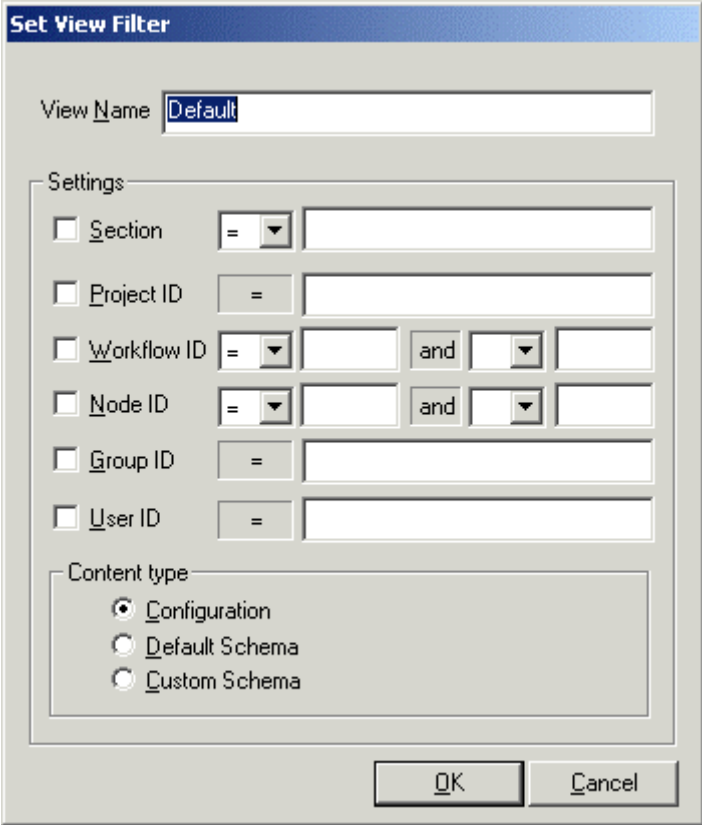
1. In the **Exigen Workflow Explorer** window, select **Administration Tools > Workflow Tools**.

2. To start Configuration Browser, double click **Configuration Browser** .

If the user has Configuration Browser access rights, the Configuration Browser is launched.

If the skip filter option is enabled, the complete current Exigen Workflow configuration appears.

If the skip filter option is not enabled, the **Set View Filter** window appears.



The **Set View Filter** dialog box is shown. It has a title bar with the text "Set View Filter". Below the title bar is a text field labeled "View Name" containing the text "Default". Below this is a section titled "Settings" containing several filter criteria, each with a checkbox, a label, an equals sign, a dropdown arrow, and a text input field:

- ☐ Section = [dropdown] [text field]
- ☐ Project ID = [text field]
- ☐ Workflow ID = [dropdown] [text field] and [dropdown] [text field]
- ☐ Node ID = [dropdown] [text field] and [dropdown] [text field]
- ☐ Group ID = [text field]
- ☐ User ID = [text field]

Below the "Settings" section is a section titled "Content type" containing three radio buttons:

- ☒ Configuration
- ☐ Default Schema
- ☐ Custom Schema

At the bottom right of the dialog box are two buttons: "OK" and "Cancel".

Figure 146: Specifying view settings

For information on the skip filter option, see [Setting User Preferences](#).

If the user does not have Configuration Browser access rights, an error message appears.

3. To grant access rights, follow instructions as described in [Specifying Security Levels](#).
4. If the **Set View Filter** window is displayed, to open the complete current Exigen Workflow configuration, click **OK**.
5. If the **Set View Filter** window is displayed, to specify a custom view, set filter values as described in [Specifying a Configuration View](#).

The configuration view appears in the **Configuration Browser** window.

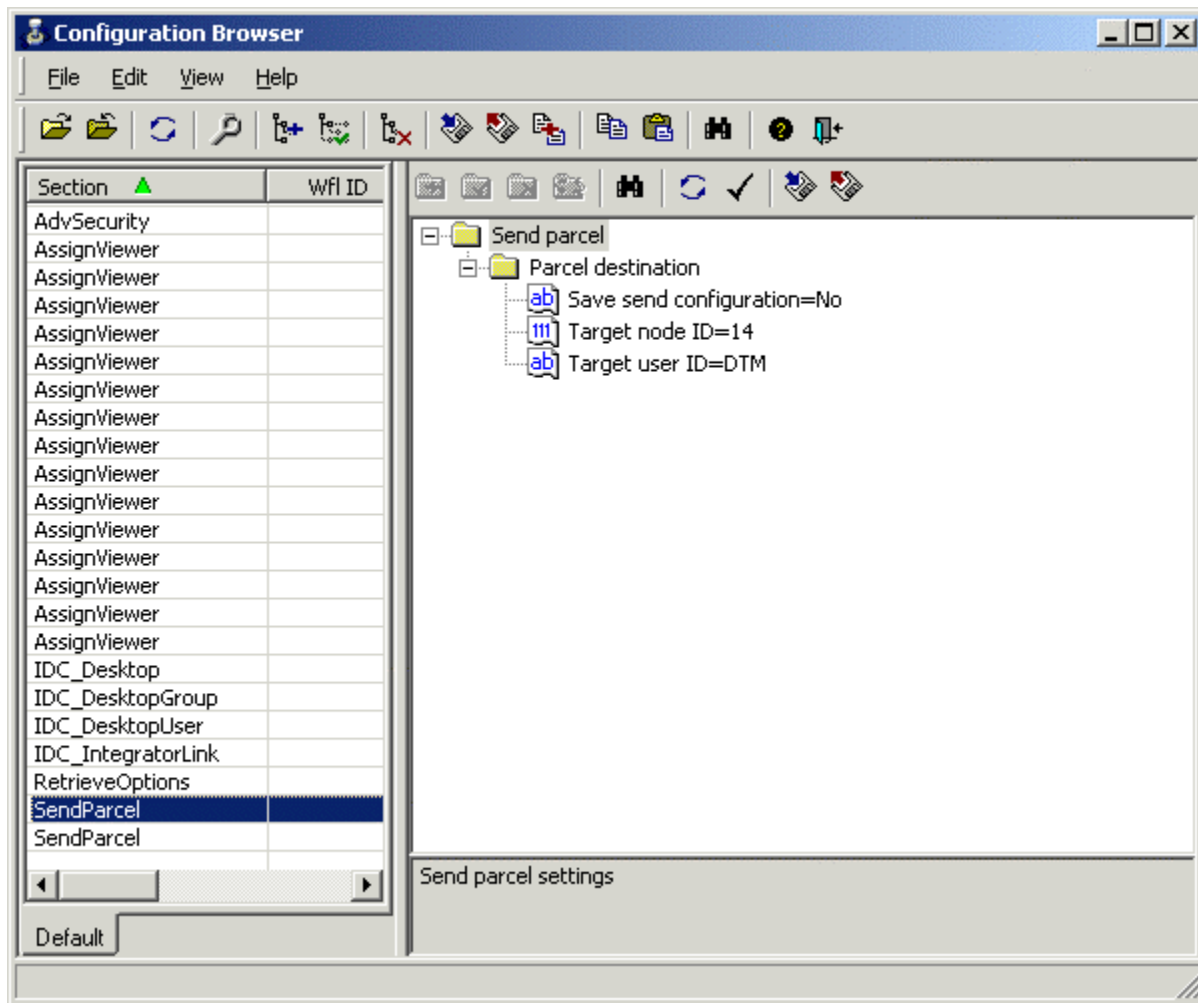


Figure 147: Opening Configuration Browser

Configuration Browser can be started if Exigen Workflow is not running. The following instructions assume that Configuration Browser is installed at the following location:

`c:\EWF\SYSTEM\MenuCfg.exe`

The preceding location is the default.

If Exigen Workflow is not running, to start Configuration Browser, proceed as follows:

1. Perform one of the following steps:
 - Run `c:\EWF\SYSTEM\MenuCfg.exe`
 - In the command line, enter `c:\EWF\SYSTEM\MenuCfg.exe`

The **Welcome to Exigen Workflow** window appears.

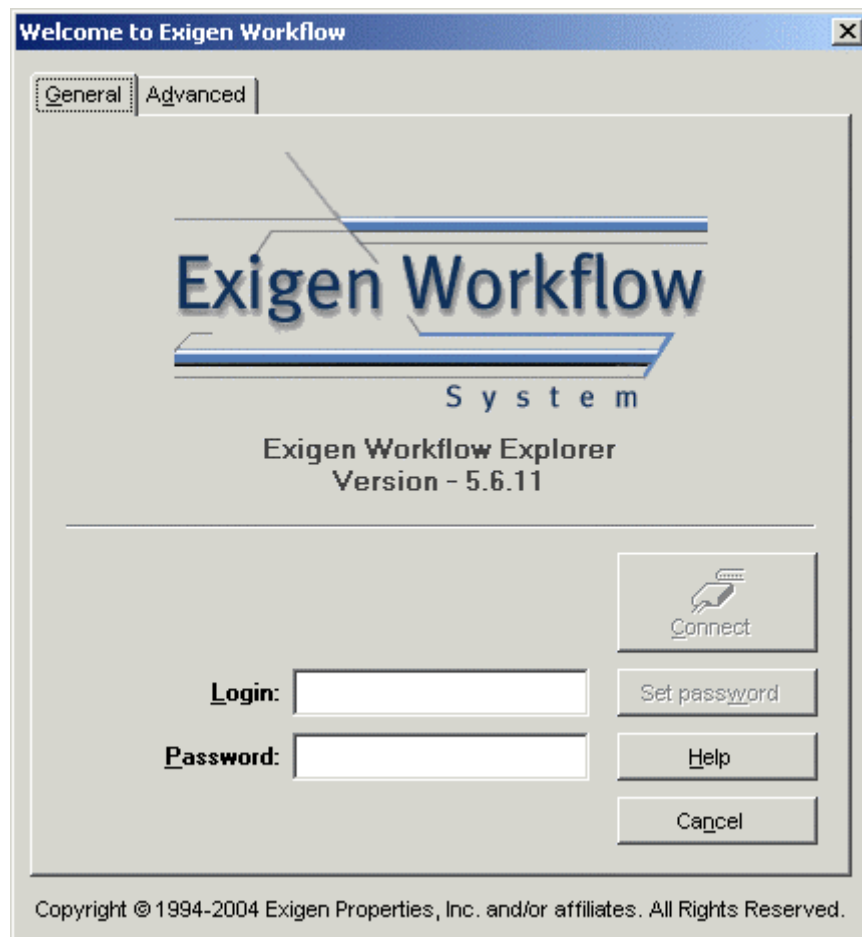


Figure 148: Starting Exigen Workflow

2. In the **Login** field, enter your Exigen Workflow user name.
3. In the **Password** field, enter your password.
4. To connect to the database, click **Connect**.

If the skip filter feature is enabled, the **Configuration Browser** window appears.


If the skip filter feature is not enabled, the **Set View Filter** window appears.

5. If the **Set View Filter** window is displayed, to open the complete current Exigen Workflow configuration, click **OK**.
6. If the **Set View Filter** window is displayed, to specify a custom view, set filter values as described in [Specifying a Configuration View](#).

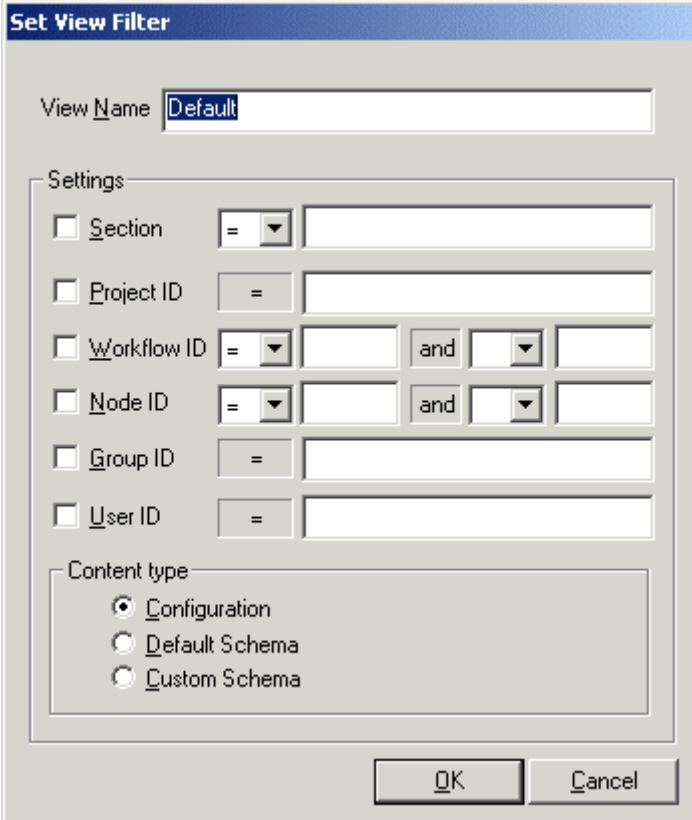
Specifying a Configuration View

The **Set View Filter** window is used to define the configuration view. For example, you can specify that only configuration sections relating to Workflow Monitor are displayed in the view.

To specify a configuration view, proceed as follows:

1. If the **Set View Filter** window is not open, to open it, click **Open View** .

The **Set View Filter** window appears.



The **Set View Filter** dialog box has a title bar with the text "Set View Filter". Below the title bar is a text field labeled "View Name" containing the text "Default". Below this is a section titled "Settings" containing several checkboxes and input fields:

- ☐ **Section**: followed by an equals sign and a dropdown arrow, and then an empty text field.
- ☐ **Project ID**: followed by an equals sign and an empty text field.
- ☐ **Workflow ID**: followed by an equals sign and a dropdown arrow, then the word "and", another dropdown arrow, and an empty text field.
- ☐ **Node ID**: followed by an equals sign and a dropdown arrow, then the word "and", another dropdown arrow, and an empty text field.
- ☐ **Group ID**: followed by an equals sign and an empty text field.
- ☐ **User ID**: followed by an equals sign and an empty text field.

Below the "Settings" section is a section titled "Content type" containing three radio buttons:

- ☒ **Configuration**
- ☐ **Default Schema**
- ☐ **Custom Schema**

At the bottom right of the dialog box are two buttons: **OK** and **Cancel**.

Figure 149: Setting a filter

2. In the **View Name** field, enter a filter name.

Entering a name is not mandatory, but is recommended. When the filter is defined, the filter name appears on a tab in the left pane.

3. To enable filters, in the **Settings** section, select the appropriate checkboxes:

Filter types	
Name	Description
Section	Configuration section.
Project ID	Project ID.
Workflow ID	Workflow ID.
Node ID	Node ID.
Group ID	Group ID.
User ID	User ID.

4. To specify values for an enabled filter, in the right part of the **Settings** section, specify a valid value.

The following search types are available:

Search types	
Name	Description
Exact	Retrieves only entries that exactly match the entire string. The = symbol is entered to specify an exact search.
Approximate	Retrieves all entries whose initial characters match the entered string. The % symbol is entered to specify an approximate search.
Greater than and less than	Specifies values greater than or less than entered values by entering > or < symbols.

- In the right part of the **Settings** section, specify the values for each filter type as follows:
 - To specify an exact search for a value, select =.
 - To specify an approximate search for a value, select %.
 - To specify a search for values greater than or less than an entered value, select the appropriate mathematical symbol, for example, >.
- Enter the search values in the appropriate fields to the right.

For example, to specify that the view display all configuration sections starting with the letters AUD, select the **Section** check box, select %, and enter *AUD* in the field to the right.

Figure 150: Specifying an approximate search

- To specify the content type, in the **Content type** field, select one of the following options:

Content type options	
Name	Description
Configuration	Allows viewing and editing the Exigen Workflow configuration.
Default Schema	Displays the default configuration schemas delivered with Exigen Workflow. Default schemas cannot be modified. For information on configuration schemas, see Managing Configuration Schemas .
Custom Schema	Displays custom configuration schemas defined by administrators. For information on configuration schemas, see Managing Configuration Schemas .

8. To save the changes and close the window, click **OK**.

To display only configuration sections with a specific value, proceed as follows:

1. In the left pane, right click a cell containing the value.
2. In the menu, select **Filter By**.

Only the configuration sections with the selected value are displayed.

For example, to view only the configuration sections that are associated with a particular user, right click the user name and select **Filter By**.

Opening a View

If a tab for the appropriate view appears in the lower part of the left pane, to open the view, click the tab.

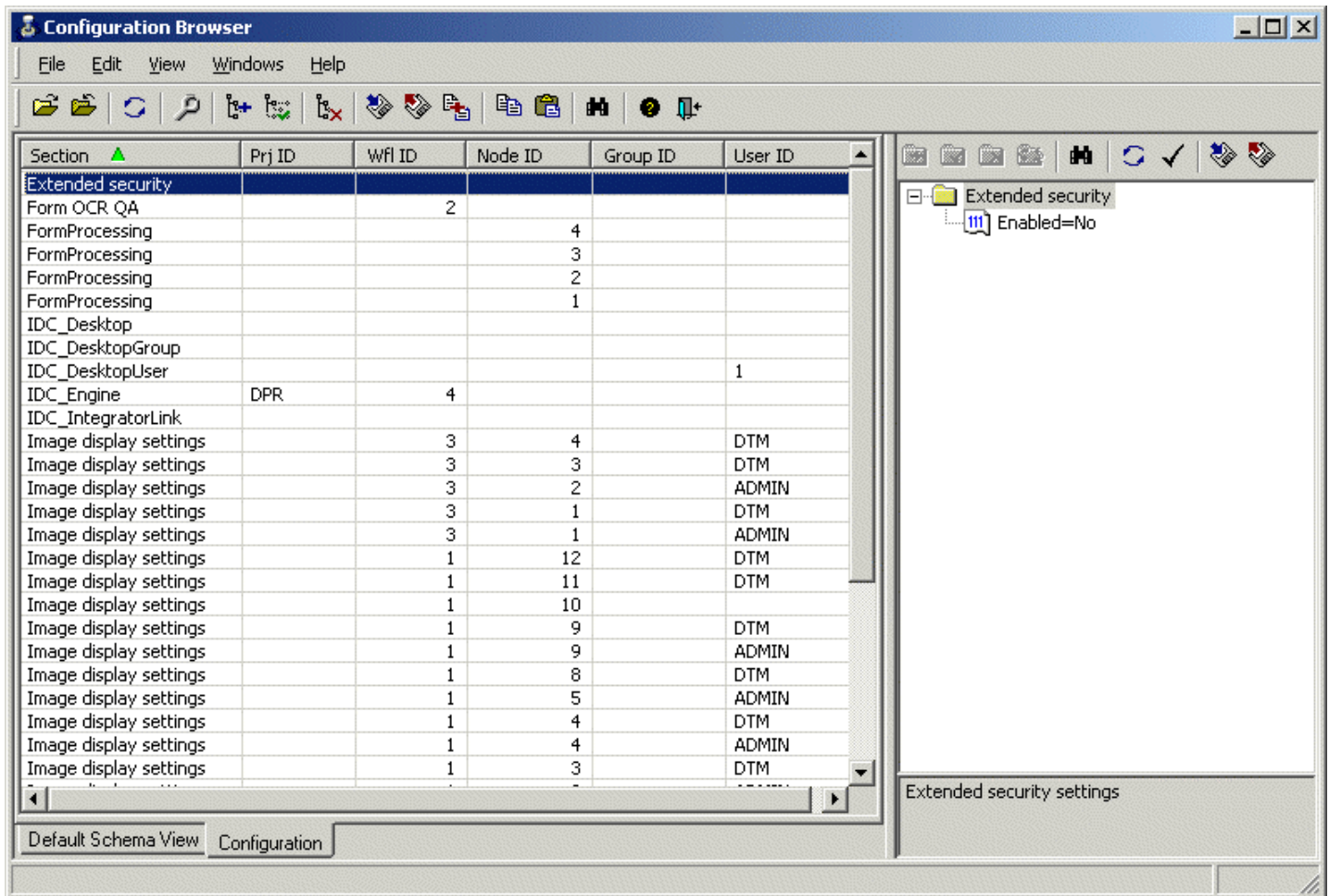



Figure 151: Opening a view using a tab

If a tab with the appropriate view is not available, to open a view, proceed as follows:

- To open the **Set View Filter** window, perform one of the following steps:
 - Click **Open View** .
 - Select **File > Open View**.
 - In the left pane, select any non-empty cell, right click, and select **Open View**.

The **Set View Filter** window appears.

- To open the complete current Exigen Workflow configuration, click **OK**.
- To specify a custom view, enter values in the **Set View Filter** window as described in [Specifying a Configuration View](#).

Closing a View

To close a view, perform one of the following steps:

- Click **Close View** .

- Select **File > Close View**.
- In the left pane, select any non-empty cell, right click, and select **Close View**.
- In the left pane, double click the tab containing the view.

Switching Between Open Views

To switch between open views, in the left pane, click the appropriate tab.

The selected view is displayed while other open views are hidden.

Refreshing a View


To refresh a view, perform one of the following steps:

- Click **Refresh Views** .
- Select **File > Refresh View**.

Adding a Configuration Section

To add a configuration section, proceed as follows:

1. Perform one of the following steps:

- Click **Add Section** .
- Select **Edit > Add Section**.
- Right click in any non-empty cell in the left pane and, in the menu, select **Add Section**.

The **New Section** window appears.

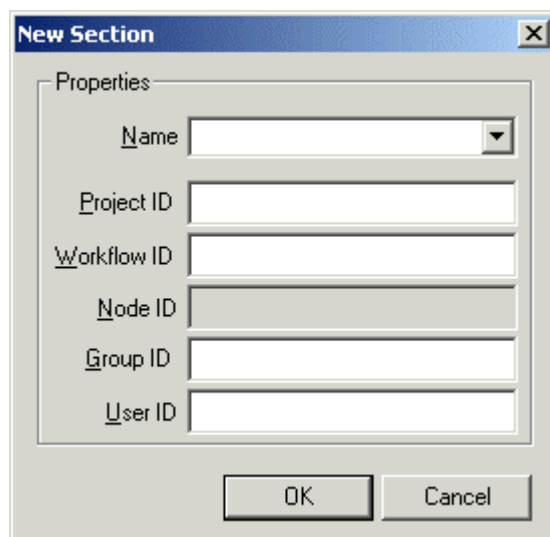


Figure 152: Adding a configuration section

2. In the fields, enter or select the appropriate values as described in the following table:

New Section window fields	
Name	Description
Name	Section name.
Project ID	Project ID. A value is entered only if the section applies to a particular project.
Workflow ID	Workflow ID. A value is entered only if the section applies to a particular workflow.
Node ID	Node ID. A value is entered only if the section applies to a particular node.
Group ID	Group ID. A value is entered only if the section applies to a particular group.
User ID	User ID. A value is entered only if the section applies to a particular user.

It is possible to create a configuration section that applies only to a particular user, node, workflow, group, or project. For example, global settings can be specified for a particular workflow. In that case, the settings apply to all users of the workflow, including administrators.


It is not possible to create two configuration sections with the same name and parameter set.

3. To save the values and close the window, click **OK**.

The new configuration section is listed in the left pane. The root node for this configuration section appears in the right pane. The configuration section and the root node have the same name.

Editing a Configuration Section

To edit the existing configuration section, proceed as follows:

1. Select the configuration section.
2. Perform one of the following steps:
 - Click **Edit Section** .
 - Select **Edit > Edit Section**.
 - Right click on any non-empty cell in the configuration section and, in the menu, select **Edit Section**.
 - Select the configuration section and press **ENTER**.

The **Edit Section** window appears.

Figure 153: Editing a configuration section

3. In the fields, modify the values.

The edited configuration section must be unique. It is not possible for two configuration sections to have the same name and parameters.


For a description of the fields in the **Edit Section** window, see [Adding a Configuration Section](#).

4. To save the changes and close the window, click **OK**.

Deleting a Configuration Section

Deleting a configuration section means deleting all nodes and values in the section.

To delete a configuration section, perform one of the following steps:

- In the left pane, right click any non-empty cell and in the menu, select **Delete Section**.
- In the left pane, select the section and select **Edit > Delete Section**.
- In the left pane, select the section and click **Delete Section** .

Adding an Item

Nodes can include one or more items. **Items** are node entries that contain values. The following is an example of an item:

```
Work start time=09:12
```

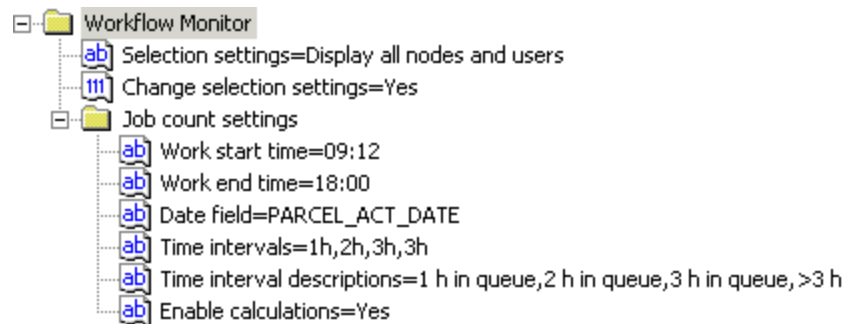



Figure 154: Items in a node

Only items that are allowed by the configuration schema can be added.

To add an item, proceed as follows:

1. In the right pane, select a node in which to add an item.
2. Perform one of the following steps:
 - Right click, select **Add**, and select an item to add.
 - Click **Add** .

If **Add** is clicked in the toolbar, the **Add new item** window appears.


3. In the **Add new item** window, in the **Item name** field, enter a value or select a value from the list box.
4. To save changes and close the window, click **OK**.

Editing an Item

Items can be edited only if it is allowed by the configuration schema. For information on edit modes, see [Setting User Preferences](#).

The procedure for editing an item depends on the user preferences specified. The following instructions are based on the assumption that none of the special edit modes are selected.

To edit an item, proceed as follows:

1. In the right pane, select an item to edit.
2. Perform any of the following steps:
 - Right click and select **Edit**.
 - Click **Edit item** .

If the value can be edited manually, it appears in a plain box.



Figure 155: Value that can be edited manually

If the value can be selected from a list, a list box appears.



Figure 156: Value that can be selected from a list

3. Enter a value manually or select a value from the list.

The icon next to the item name indicates the type of value that can be entered. For information on item icons, see [Configuration Browser User Interface](#).


4. To continue work without saving the value, click any other item or section.
5. To undo the most recent modification, reload the configuration for the item as described in [Undoing Unsaved Modifications](#).
6. To save the new value, press **ENTER** or click **Apply** .

The new value is saved.

Renaming an Item

Only child items of custom items can be renamed.

To rename an item, proceed as follows:

1. In the right pane, select an item to edit.
2. Click **Rename** .

The **Rename item** window appears.

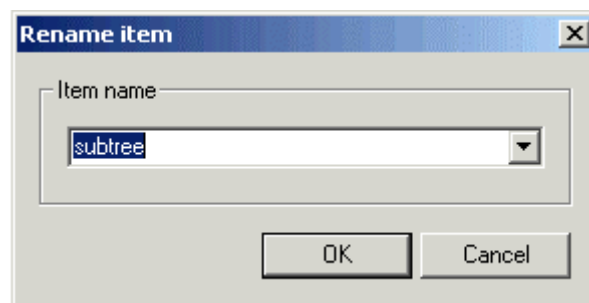


Figure 157: Renaming an item

3. In the **Rename item** window, enter a new name for the item.
4. To close the window and save changes, click **OK**.

Undoing Unsaved Modifications

To undo the most recent unsaved modifications in the right pane, perform one of the following steps:


- Click **Refresh** .
- In the right pane, right click and select **Refresh**.

Configuration data is updated from the database.

Deleting an Item

Items can be deleted only if allowed by the configuration schema.

To delete an item, proceed as follows:



1. Select the item.
2. Perform one of the following steps:
 - Click **Delete** .
 - Press **Delete**.
3. In the **Delete confirmation** window, click **Yes**.

Copying and Pasting a Configuration Section

In Configuration Browser, each configuration section must be unique. Two configuration sections cannot have the same name and parameter set.

For this reason, copied configuration sections are edited before pasting them into the configuration.

To copy and paste a configuration section, proceed as follows:

1. In the left pane, select a configuration section to copy.
2. To copy the section, perform one of the following steps:
 - Click **Copy Configuration** .
 - Select **Edit > Copy Configuration**.
 - Right click and select **Copy Configuration**.
3. To paste the section, perform any of the following steps:
 - Click **Paste Configuration** .
 - Select **Edit > Paste Configuration**.
 - Right click on any non-empty cell in the left pane and select **Paste Configuration**.

The **New Section** window appears.

4. In the **New Section** window, modify one or more values.

For information on the fields in the **New Section** window, see [Adding a Configuration Section](#).

5. Click **OK**.

The new section appears.

Exporting a View

A view can be exported as a file with a `.cfg` extension. The exported file contains configuration context information such as user ID, node ID, workflow ID, and project ID.

To export a view, proceed as follows:

1. Open a view to export.

For information on opening a view, see [Opening a View](#).

2. Select **File > Export View**.
3. In the **Save As** window, specify a location and file name for saving the exported view.
4. To save the file, click **Save**.

The view is saved as a `.cfg` file.

Exporting a Configuration Section

A configuration section can be exported as a `.cfg` file. The exported file contains configuration context information such as user ID, node ID, workflow ID, and project ID.

To export a configuration section, proceed as follows:

1. In the left pane, select a configuration section to export.
2. To export the configuration section, perform one of the following steps:
 - In the left pane, right click and select **Export Section(s)**.
 - Select **Edit > Export Section(s)**.
3. In the **Save As** window, select a location and file name for export.
4. Click **Save**.

The configuration section is saved as a `.cfg` file.

Importing a Configuration Section

A configuration section that was exported as a `.cfg` file can be imported.

For information on exporting configuration sections, see [Exporting a Configuration Section](#).

To import a configuration section, proceed as follows:

1. To initiate the import process, perform one of the following steps:
 - Select **Edit > Import Section(s)**.
 - In the left pane, right click any non-empty cell and select **Import Section(s)**.
2. In the **Open** window, select a file to import.

The file must have a `.cfg` extension.

3. Click **Open**.

The **Select sections to import** window appears.

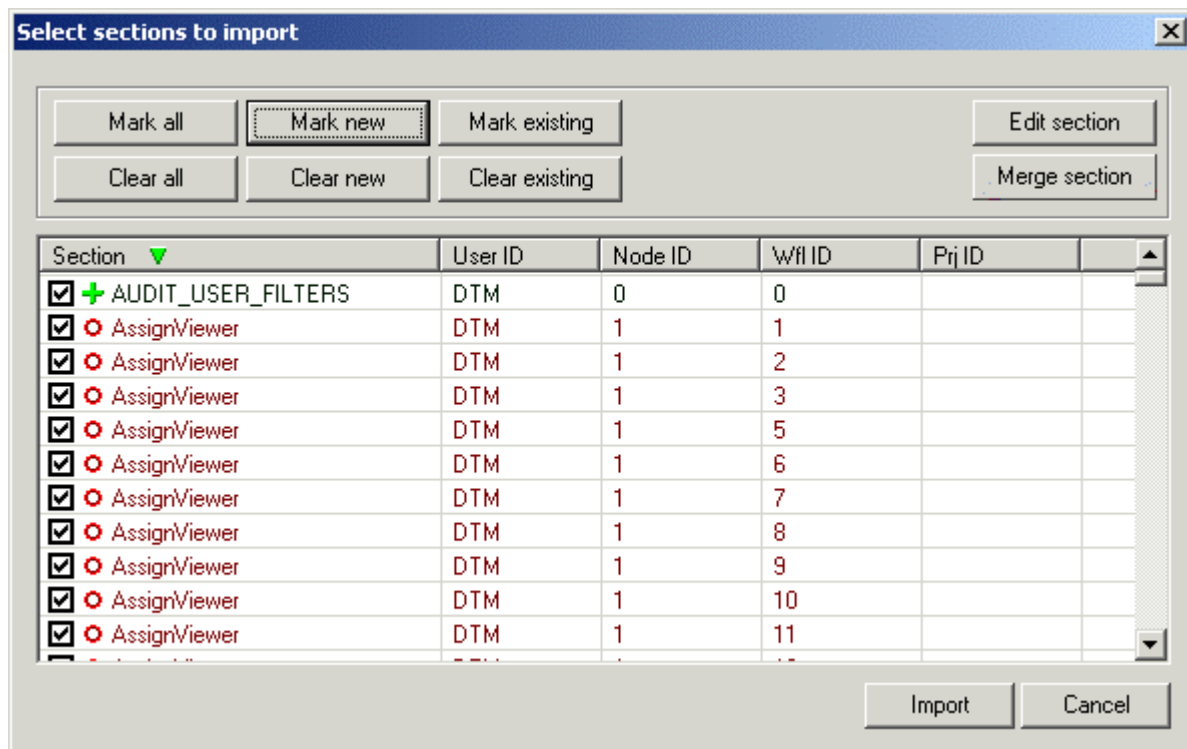


Figure 158: Selecting sections to import

The **Select sections to import** window displays a list of sections in the import file and the attributes of each section. The following table describes the symbols assigned to sections:

Section symbols	
Symbol	Description
	Section does not exist in the current configuration. If the section is selected for import, it is imported as a new section.
	Section exists in the current configuration. If the section is selected for import, it overwrites an existing section.
<input checked="" type="checkbox"/>	Section is selected for import.
	Section that was modified during merge section process. If the section is selected for import, it overwrites an existing section.

- To clear all sections in the import file, click **Clear all**.
- To select all sections for import, click **Mark all**.
- To select all sections that do not exist in the current configuration, click **Mark new**.
- To clear all sections that do not exist in the current configuration, click **Clear new**.
- To select all sections that exist in the current configuration, click **Mark existing**.
- To clear all sections that exist in the current configuration, click **Clear existing**.
- To select individual sections for import, select the appropriate check boxes.

11. To edit a section prior to import, select the section and click **Edit section**.

The **Edit Section** window appears.

12. Edit the section as described in [Editing a Configuration Section](#).
13. To edit a configuration file prior to import, click **Merge**.

If a file-editing application is specified, it is launched. For information on specifying an application, see [Specifying an Application for Merging Configurations](#).

14. In the file-editing application, make appropriate changes in the file to be imported.
15. Save the changes and close the file-editing application.
16. To import all selected sections and close the window, click **Import**.



The sections are imported into the configuration.

Exporting and Importing Configuration Data

Selected configuration data can be exported to a file in `.xml` format and imported into the configuration. The imported data is used to create a new configuration section. The user provides parameters for the new configuration section.

It is also possible to import a configuration template file in `.txt` format.

To export and import configuration data, proceed as follows:

1. In the left pane, select a section to export.
2. To export the configuration data, perform one of the following steps:
 - Click **Export Configuration** .
 - Select **Edit > Export Configuration**.
3. In the **Save As** window, select a file name and location to save the `.xml` file.
4. To save the file, click **Save**.
5. To import configuration data, perform one of the following steps:
 - Click **Import Configuration** .
 - Select **Edit > Import Configuration**.
6. To import an `.xml` file, in the **Files of type** window, select **Configuration exports (*.xml)**.
7. To import a configuration template, in the **Files of type** window, select **Configuration template (*.txt)**.
8. Select the file to import.
9. To import the file, click **Open**.
10. If the **New Section** window appears, modify one or more values.

For information on the fields in the **New Section** window, see [Adding a Configuration Section](#).



11. Click **OK**.

The new section appears.

Exporting and Importing a Configuration Node

A configuration node can be exported as an `.xml` file and imported as a child node of a selected node. Importing a node is possible only if it is allowed by the configuration schema.

To export and import a configuration node, proceed as follows:

1. In the right pane, select a configuration node to export.
2. To export the configuration, perform one of the following steps:
 - In the right toolbar, click **Export** .
 - Right click the node and select **Export**.
3. In the **Save As** window, select a file name and location to save the `.xml` file.
4. To save the file, click **Save**.
5. In the left pane, select a configuration section for the new child node.
6. In the right pane, select a parent node for the new child node.
7. To import the configuration, perform one of the following steps:
 - In the right toolbar, click **Import** .
 - Right click the parent node and select **Import**.
8. In the **Open** window, select the `.xml` file to import.
9. To import the file, click **Open**.

The file is imported.


Merging Configurations

The following types of configuration merges are performed in Configuration Browser:

- A current Configuration Browser configuration is merged with a configuration file using a file-merging application.
- Configuration sections are imported and merged into a current configuration using a file-merging application.

If a file-merging application is used in the merge process, the application must be specified. For information on specifying an application, see [Specifying an Application for Merging Configurations](#).

To merge a current Configuration Browser configuration with a configuration file in an external application, proceed as follows:

1. To initiate the merge process, perform one of the following steps:
 - Click **Merge configuration** .
 - In the **Section** column, right click and select **Merge Configuration**.

The **Open** window appears.

2. Select a configuration file to merge.
3. Click **Open**.

The file-merging application is launched. It displays the external configuration and the current Configuration Browser configuration. The name `browser` is appended to the name of the current Configuration Browser configuration.

4. In the file-merging application, edit the merged configuration as required and save changes.

For information on editing the configuration and saving changes, see the documentation for the file-merging application.

5. If an error message appears, to revoke the configuration changes, click **Cancel**.
6. If an error message appears, to reopen the file-merging application and make changes, click **OK**.
7. Make appropriate changes in the configuration.
8. Save the changes and close the file-merging application.

All changes that are saved in the file-merging application are saved automatically in Configuration Browser.

For information on merging configurations using the import process, see [Importing a Configuration Section](#).

Setting User Preferences

The following topics are described in this section:

- [Specifying Settings for Editing Values](#)
- [Specifying an Application for Merging Configurations](#)
- [Hiding and Displaying the Set View Filter Window](#)
- [Specifying Section Sorting Order](#)
- [Specifying Default Settings for Hiding and Displaying Section Columns](#)

Specifying Settings for Editing Values

In Configuration Browser, the user can specify settings for editing values.

The following edit modes are available:

Edit modes	
Mode	Description
Hotkey	Activated when F2 or ENTER is pressed.
Auto	Activated when an item is selected. This mode overrides other edit modes, which are unavailable when Auto is selected.
Anykey	Activated when an item is selected and an acceptable key for the value is pressed. For example, if the item Target node ID requires a numerical value, entering a number activates the edit mode, but entering a letter does not.

Edit modes	
Mode	Description
Auto commit	Modified value is saved when a new item is selected.

To set Configuration Browser edit modes, proceed as follows:

- To open the window for specifying user preferences, perform one of the following steps:

- Click **Edit Preferences** .
- Select **File > Edit Preferences**.

In the right pane, the **Configuration browser preferences** tree appears.

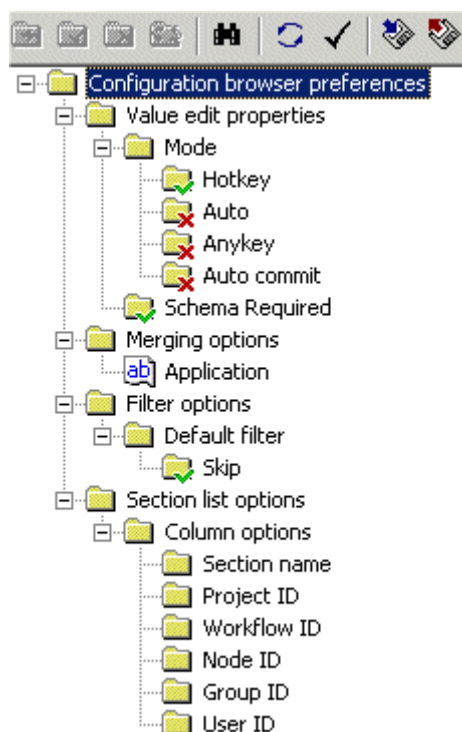


Figure 159: Specifying user settings

- To enable edit modes, in the **Mode** folder, click the appropriate subfolders.

A green check mark indicates that a mode is activated.



A red X indicates that a mode is not activated.



The settings are saved automatically.


- To enable or disable the ability to modify sections without schemas, click the **Schema Required** folder.

4. To close the **Configuration browser preferences** tree and continue working with Configuration Browser, open a view as described in [Opening a View](#).

Specifying an Application for Merging Configurations

Configurations can be merged using a file-merging utility such as Araxis Merge or WinDiff.

To specify an application for merging configurations, proceed as follows:

1. In the **Configuration browser preferences** tree, in the **Merging options** subfolder, right click **Application**.
2. Select **Edit**.
3. To select the file-merging utility, click the browse button .

The **Open** window appears.


4. Select the application and click **Open**.
5. To save the setting, press **ENTER** or click **Apply**.

Hiding and Displaying the Set View Filter Window

The user can specify whether the **Set View Filter** window is hidden or displayed when Configuration Browser is started.

To hide or display the **Set View Filter** window, proceed as follows:

1. In the **Configuration browser preferences** tree, locate the **Default filter** subfolder.

If the skip filter option is enabled, a checkmark appears:  Skip .

If the skip filter option is not enabled, an X appears:  Skip .

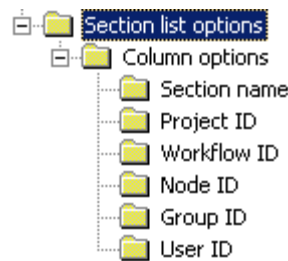
2. To reverse the state of the skip filter option, click the **Skip** folder.

If the skip filter option was enabled, it is disabled. If the skip filter option was disabled, it is enabled.

Specifying Section Sorting Order

To specify the default order in which section columns are displayed, proceed as follows:

1. In the **Configuration browser preferences** tree, locate the **Section list options** subfolder.




The **Column options** subfolder lists the section columns that appear in the Configuration Browser left pane. The column name listed at the top of the **Column options** subfolder corresponds to the column at the far left of the Configuration Browser left pane.


2. To move a section column up in the sorting order, select the appropriate column name, and press **ALT** and the upward arrow key.
3. To move a section column down in the sorting order, select the appropriate column name, and press **ALT** and the downward arrow key.

Specifying Default Settings for Hiding and Displaying Section Columns

To hide a column in all configuration sections by default, perform one of the following steps:


- In the **Configuration browser preferences** tree, in the **Column options** subfolder, select the column name and click **Delete** .
- In the **Configuration browser preferences** tree, in the **Column options** subfolder, right click the column name and select **Delete**.

To redisplay a column that is hidden by default, perform one of the following steps:

- In the **Configuration browser preferences** tree, right click the **Column options** subfolder, select **Add**, and select the column name.
- In the **Configuration Browser** window right pane, click **Add** , select a name in the **Item Name** field, and click **OK**.

Searching for Items or Values in a Configuration Section

To search for an item or value in a configuration section, proceed as follows:

1. In the left pane, select the configuration section.
2. To open the **Find item** window, in the right toolbar, click **Find**  or press **CTRL+F**.

The **Find item** window appears.

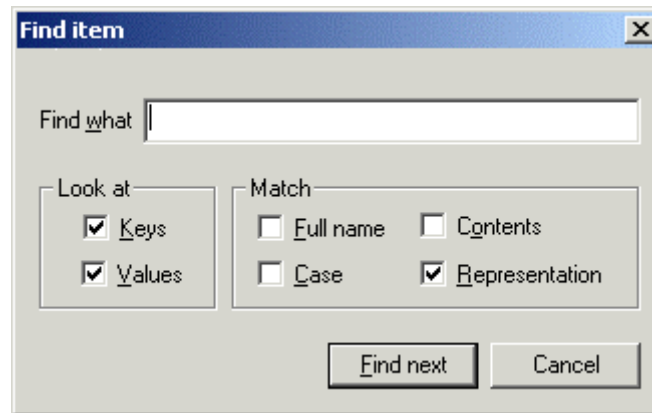


Figure 160: Searching for a value or item

- To define the search, in the **Find item** window, select the appropriate options and enter the appropriate values as described in the following table:


Find item window elements	
Name	Description
Find what	Full string or start of the string to search for. It can include letters, numbers, or both. For example, if the search is for items starting with the name AUDIT, <i>AUDIT</i> is entered.
Look at	If Keys is selected, search includes item names. If Values is selected, search includes values.
Match	If Full name is selected, returns only items containing the same set and number of characters as the entered string. For example, a search for <i>AUTO</i> returns <i>AUTO</i> , but does not return <i>AUTOMOBILE</i> . If Case is selected, only items matching the string and having the same uppercase and lowercase letters are returned. For example, a search for <i>AUTO</i> returns <i>AUTO</i> , but not <i>auto</i> . If Contents is selected, the search returns values and items in the database. If Representation is selected, the search returns only values and items displayed in Configuration Browser.

- To start the search, click **Find next**.
- To close the window without searching, click **Cancel**.

Searching for Items or Values in Multiple Configuration Sections

To search for items or values in multiple configuration sections, proceed as follows:

- If the search does not include all configuration sections, in the left pane, select the sections to be searched.
- To initiate the search, perform one of the following steps:

- Select **Edit > Find Item**.
- In the selected sections, right click any non-empty cell and select **Find item**.
- In the left pane, click **Find** .

The **Find item** window appears.

3. To search only selected sections, select **Selected sections**.
4. To search all sections, select **All sections**.
5. To define search options and perform the search, follow instructions as described in [Searching for Items or Values in a Configuration Section](#), steps 3 through 5.

Sorting Items in the Configuration View

To sort the items in a column, click the column name.

For example, clicking the **Node ID** column sorts the configuration sections based on node ID in ascending or descending order.

Multisort selection is used to sort columns based on multiple values.

To activate multisort selection, proceed as follows:

1. In the left pane, right click any column name and select **Start multisort selection**.
2. Click on the columns to include in the multisort selection.

To invert the multisort selection, in the left pane, right click any column name and select **Invert multisort selection**. For example, if the columns are initially sorted in ascending order, they are resorted in descending order.

To cancel multisort selection, in the left pane, right click any column name and select **Cancel multisort selection**.

Displaying and Hiding Columns in the Configuration View

To hide a column in the configuration view, right click the column and select **Hide column**.

Note: The **Section** column cannot be hidden.


To display a hidden column, proceed as follows:

1. Right click on any column name.
2. Select **Columns**.
3. Click the name of the column to be displayed.

To specify that columns be hidden in all configuration sections by default, proceed as described in [Specifying Default Settings for Hiding and Displaying Section Columns](#).

Exiting Configuration Browser

To exit Configuration Browser, perform one of the following steps:

- Click **Exit** .
- Select **File > Exit**.
- Press **F12**.

Managing Configuration Schemas

A **configuration schema** defines the structure and available items for a configuration section. When an administrator creates a new configuration section, an appropriate configuration schema can be selected. Only those configuration parameters and items that are defined in the schema can be used in the configuration section.

There are the following configuration schema types:

Configuration schema types	
Type	Description
Default	Fixed configuration structure that is defined in the system and cannot be modified.
Custom	Additional configuration structure that is created by an administrator. Custom schemas can be modified.

Both types of configuration schemas are available to the administrator when creating a new configuration section.

The following topics are described in this section:

- [Viewing Configuration Schemas](#)
- [Creating a New Configuration Schema](#)
- [Modifying a Configuration Schema](#)
- [Deleting a Configuration Schema](#)

Viewing Configuration Schemas

To view a configuration schema, proceed as follows:

1. In the **Configuration Browser** window, click **Open View** .

The **Set View Filter** window appears.

2. In the **View Name** field, enter an appropriate view name.
3. In the **Content type** box, select one of the following options as required:
 - To open the default configuration schema, select the **Default Schema** option.
 - To open the custom configuration schema, select the **Custom Schema** option.

Configuration schemas are displayed on the left. The configuration of the selected schema is displayed on the right.

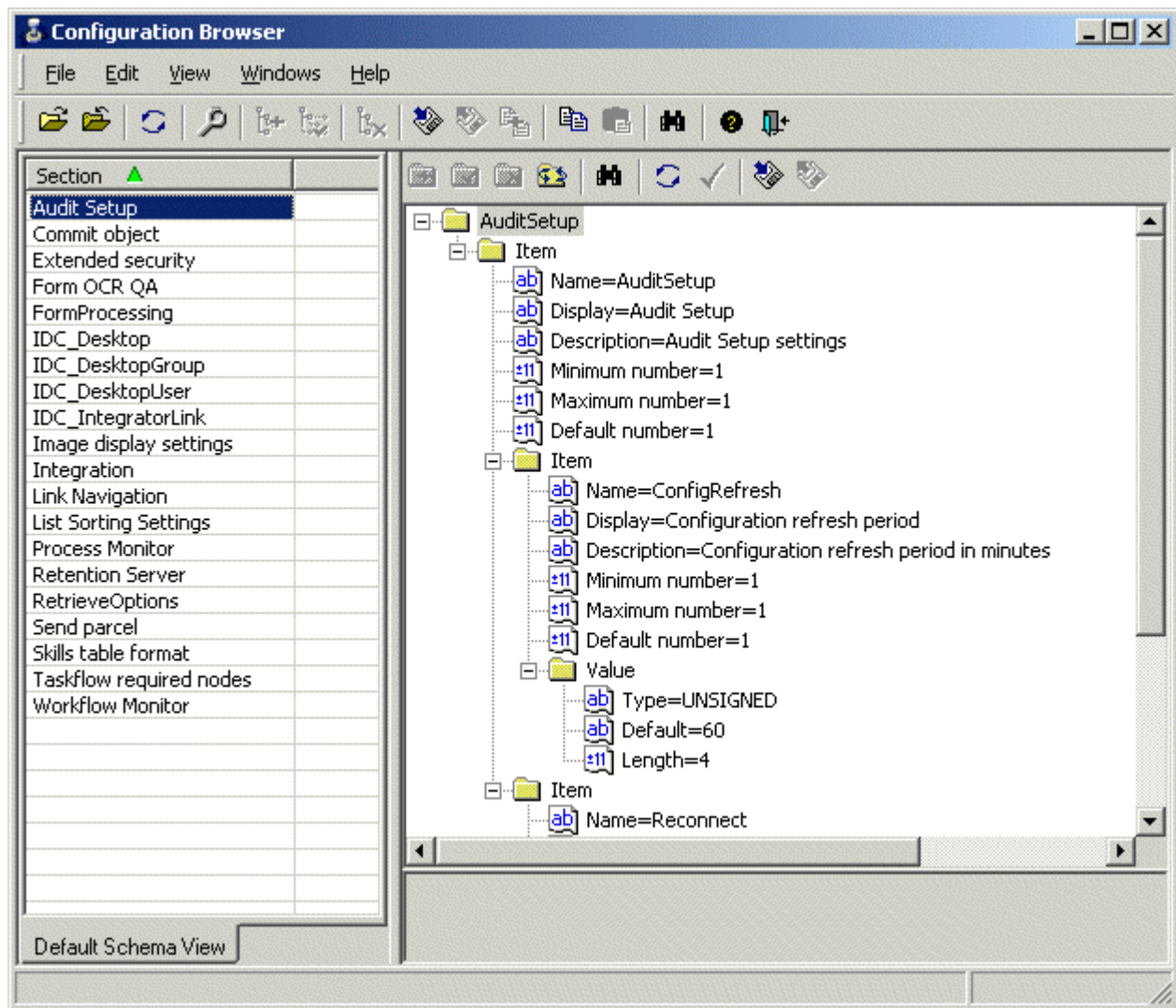



Figure 161: Viewing a configuration schema

Creating a New Configuration Schema

Only custom configuration schemas can be added. Default configuration schemas cannot be modified.

The process of creating a configuration schema is similar to creating a configuration section. For information on creating a configuration section, see [Adding a Configuration Section](#).

To create a new configuration schema, proceed as follows:

1. Open the custom configuration schema view as described in [Viewing Configuration Schemas](#).
2. Click **Add Section** .

The **New Section** window appears.

3. In the **Name** field, enter the name of the new configuration schema and click **OK**.

A new configuration schema is created with one subfolder named **Item** containing default parameters.

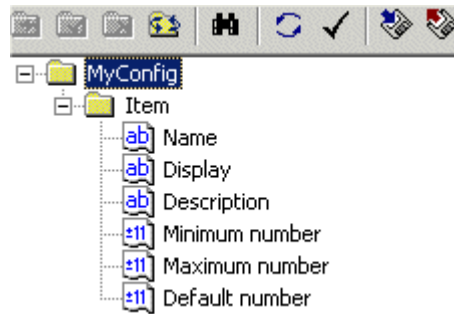



Figure 162: New configuration schema with default items

This item is named the **root item** and it contains general information about the configuration schema. The root item can contain subitems to represent specific configuration parameters.

4. Configure the **Name** parameter so that its value is the same as the name of the configuration schema.

For example, if the name of the configuration schema is *MyConfig*, the value of the **Name** parameter must also be *MyConfig*.

5. For the **Display** parameter, create a value that represents the configuration schema name displayed to the administrator.
6. For the **Description** parameter, create a value that represents the configuration schema description.
7. For the following parameters, set the values to 1:
 - **Minimum number**
 - **Maximum number**
 - **Default number**

8. To create a subitem, select the root item and click **Add** .













For information on creating configuration items, see [Adding an Item](#).


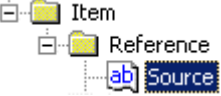
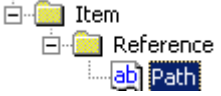

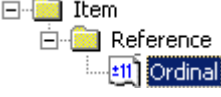



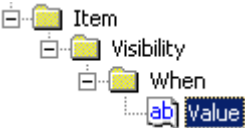

The **Add new item** window appears.

9. In the **Item name** list box, select **Item**.

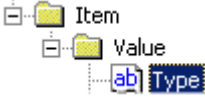
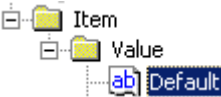


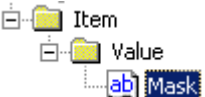

A new subitem with default parameters is created.



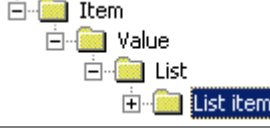


10. Configure the subitem parameters and add new parameters as described in the following table:

Configuration schema parameters	
Parameter	Description
	<p>Item name.</p> <p>The * character can be used as a substitute for any set of characters at the end of the string.</p> <p>For example, if the Name value is set to Var*, the system recognizes configuration items Var1, Var12, and VarABC for the configuration section that is based on the current schema.</p>
	<p>Item name displayed to the administrator.</p> <p>If this parameter is not defined, the Name parameter value is displayed.</p>
	<p>Item description.</p>
	<p>Minimum required number of items of the same kind.</p>
	<p>Maximum number of items of the same kind that can be defined in the configuration section.</p>
	<p>Initial number of items created automatically when the configuration section is created.</p>
	<p>Switch that defines if configuration schema settings apply to the children of this item.</p> <p>If the check mark is visible, administrators can freely customize child items.</p>
	<p>Switch that defines if the configuration item is a toggle parameter.</p> <p>Toggle parameters are suitable for parameters that can have only two values, usually on or off. The value of a toggle parameter can be changed by clicking the parameter icon. The parameter is switched on and has the value 1 when the check mark is visible. The parameter is switched off and has the value 0 when the X is visible.</p>
	<p>Switch that defines if this item can be modified.</p> <p>If the check mark is visible, administrators can only view this item but not modify it.</p>
	<p>Parameter that contains information about a custom icon that must represent this item in Configuration Browser.</p> <p>The icon can be either acquired from the owner application or retrieved from a dynamic link library.</p>
	<p>Name of the file that contains the custom icon.</p> <p>If this parameter is not specified, the icon is requested from the parent application.</p>
	<p>Icon index in the file.</p>

Configuration schema parameters									
Parameter	Description								
	<p>Parameter that defines that the configuration schema for this item must be taken from another source.</p> <p>If this parameter is specified, all other parameters in this item are ignored.</p>								
	<p>Source type from which the configuration schema for this item is taken.</p> <p>The following values are available:</p> <table> <tr> <th>Source</th><th>Description</th></tr> <tr> <td>schema</td><td>Data must be taken from the current schema.</td></tr> <tr> <td>owner</td><td>Data must be taken from the owner of the configuration editor control.</td></tr> <tr> <td>dll</td><td>Data must be taken from a DLL file.</td></tr> </table>	Source	Description	schema	Data must be taken from the current schema.	owner	Data must be taken from the owner of the configuration editor control.	dll	Data must be taken from a DLL file.
Source	Description								
schema	Data must be taken from the current schema.								
owner	Data must be taken from the owner of the configuration editor control.								
dll	Data must be taken from a DLL file.								
	<p>Path to the configuration source.</p> <p>The interpretation of the value depends on the selected source type. If the schema source type is selected, the value contains a path to the configuration item whose configuration must be used. If the dll source type is selected, the value contains the name or full path of the dynamic link library containing the configuration data.</p>								
	<p>Name of the procedure to be called in the specified DLL file if the dll source type is selected.</p>								
	<p>Ordinal of the procedure to be called in the specified DLL file if the dll source type is selected.</p> <p>This parameter is used only if the procname parameter is not specified.</p>								
	<p>Collection of rules that define the conditions when this item is visible to administrators.</p> <p>The condition is defined by the value of another configuration item.</p>								
	<p>Container of parameters that define item visibility conditions.</p> <p>The Visibility parameter can contain multiple When parameters.</p>								
	<p>Full path to the item whose value must be checked for visibility.</p>								
	<p>Value to be checked for visibility.</p> <p>If the value of the configuration item specified in the Source parameter matches the value of this parameter, the configuration item is visible to administrators.</p>								
	<p>Collection of parameters that define the value of this configuration item.</p>								

Configuration schema parameters

Parameter	Description																
	<p>Value data type.</p> <p>The following types are available:</p> <table> <tr> <th>Type</th><th>Description</th></tr> <tr> <td>VARCHAR</td><td>String value.</td></tr> <tr> <td>INTEGER</td><td>Signed integer value.</td></tr> <tr> <td>UNSIGNED</td><td>Unsigned integer value.</td></tr> <tr> <td>FLOAT</td><td>Signed floating number.</td></tr> <tr> <td>DATETIME</td><td>Date and time value in the following format: YYYY/MM/DD hh:mm:ss</td></tr> <tr> <td>DATE</td><td>Date value in the following format: YYYY/MM/DD</td></tr> <tr> <td>TIME</td><td>Time value in the following format: hh:mm:ss</td></tr> </table>	Type	Description	VARCHAR	String value.	INTEGER	Signed integer value.	UNSIGNED	Unsigned integer value.	FLOAT	Signed floating number.	DATETIME	Date and time value in the following format: YYYY/MM/DD hh:mm:ss	DATE	Date value in the following format: YYYY/MM/DD	TIME	Time value in the following format: hh:mm:ss
Type	Description																
VARCHAR	String value.																
INTEGER	Signed integer value.																
UNSIGNED	Unsigned integer value.																
FLOAT	Signed floating number.																
DATETIME	Date and time value in the following format: YYYY/MM/DD hh:mm:ss																
DATE	Date value in the following format: YYYY/MM/DD																
TIME	Time value in the following format: hh:mm:ss																
	Default value assigned to the configuration item when it is created.																
	<p>Switch that enables or disables an additional button in the configuration section for this item.</p> <p>The button must be handled by the parent application. It is useful for opening dialogs, such as the open file dialog.</p>																
	Maximum value length for the VARCHAR data type.																
	<p>Value mask for the date and time data type.</p> <p>The following elements can be used to construct the date and time mask:</p> <table> <tr> <th>Element</th><th>Description</th></tr> <tr> <td>yyyy</td><td>Years.</td></tr> <tr> <td>MM</td><td>Months.</td></tr> <tr> <td>dd</td><td>Days.</td></tr> <tr> <td>HH</td><td>Hours in 24 hour format.</td></tr> <tr> <td>mm</td><td>Minutes.</td></tr> <tr> <td>ss</td><td>Seconds.</td></tr> </table> <p>Any text that is to be used in its exact form in the date value must be enclosed between single quotation marks in the mask string. The single quotation mark can also be used as an escape character to allow the single quotation mark itself to be displayed in the date string.</p>	Element	Description	yyyy	Years.	MM	Months.	dd	Days.	HH	Hours in 24 hour format.	mm	Minutes.	ss	Seconds.		
Element	Description																
yyyy	Years.																
MM	Months.																
dd	Days.																
HH	Hours in 24 hour format.																
mm	Minutes.																
ss	Seconds.																
	Collection of parameters that define available values that can be selected from a list.																

Configuration schema parameters	
Parameter	Description
	<p>Switch that controls the ability to set a value manually without picking a value from the list.</p> <p>If the check mark is visible, the administrator can select only those values that are available in the list.</p>
	<p>List sorting switch.</p> <p>If the check mark is visible, the list of available values is sorted.</p>
	<p>Collection of parameters that define a list item available for selection.</p> <p>A list can have multiple list items.</p>
	List item value.
	List item value that is displayed to the administrator.

11. Add as many subitems as required in the configuration schema.

Subitems can also contain subitems.

The new configuration schema is available for selection when creating a new configuration section.

Modifying a Configuration Schema

Only custom configuration schemas can be modified.

To modify a configuration schema, proceed as follows:

1. Open the custom configuration schema view as described in [Viewing Configuration Schemas](#).
2. In the list on the left side, select the configuration schema.
3. On the right side, add, modify, or delete configuration parameters as required.

For information on configuration parameters, see [Creating a New Configuration Schema](#).

Deleting a Configuration Schema

Only custom configuration schemas can be deleted.

To delete a configuration schema, proceed as follows:

1. Open the custom configuration schema view as described in [Viewing Configuration Schemas](#).

2. In the list on the left side, select the configuration schema.

3. Click **Delete Section** .

A confirmation window appears.

4. In the confirmation window, click **Yes**.

Configuration Browser Menu Commands and Buttons

The following topics are described in this section:

- [Menu Commands](#)
- [Left Toolbar Buttons](#)
- [Right Toolbar Buttons](#)

Menu Commands














The following table lists Configuration Browser menu commands:



Configuration Browser menu commands			
Menu	Menu command	Shortcut key	Description
File	Open View		Opens a configuration view.
	Close View		Closes the current view.
	Refresh View		Refreshes the view with the latest information from the Exigen Workflow database.
	Export View		Exports the current view.
	Edit Preferences		Sets Configuration Browser user preferences.
	Exit	F12	Exits Configuration Browser.
Edit	Add Section		Adds a section to the configuration.
	Edit Section		Edits the selected configuration section.
	Delete Section(s)		Deletes the selected configuration sections.
	Export Section(s)		Exports the selected configuration sections.
	Import Section(s)		Imports the selected configuration sections.
	Export Configuration		Exports configuration data as an .xml file.
	Import Configuration		Imports configuration data from the selected .xml file.

Configuration Browser menu commands			
Menu	Menu command	Shortcut key	Description
	Merge Configuration		Launches an application used to merge external configuration data into the current configuration.
	Copy Configuration		Copies the configuration section to the clipboard.
	Paste Configuration		Pastes the configuration section from the clipboard.
	Find Item		Initiates a search in configuration sections.
View	Toolbar		Displays or hides the toolbar.
	Status Bar		Displays or hides the status bar.
Help	Context Help	F1	Opens context help.
	Help Topics	CTRL+F1	Opens a list of help topics.
	About Configuration Browser		Displays information on the Exigen Workflow version and the workstation ID.

Left Toolbar Buttons










The left toolbar contains the following buttons:

Configuration Browser left toolbar buttons		
Icon	Name	Description
	Open View	Opens a configuration view.
	Close View	Closes the current view.
	Refresh Views	Refreshes the view with the latest information from the Exigen Workflow database.
	Edit Preferences	Sets Configuration Browser user preferences.
	Add Section	Adds a configuration section.
	Edit Section	Edits the selected configuration section.
	Delete Section	Deletes the selected configuration section.
	Export Configuration	Exports configuration data as an .xml file.
	Import Configuration	Imports configuration data from an .xml file.
	Merge Configuration	Launches an application used to merge external configuration data into the current configuration.
	Copy Configuration	Copies the selected configuration section.
	Paste Configuration	Pastes the selected configuration section.
	Find	Initiates a search in configuration sections.

Configuration Browser left toolbar buttons		
Icon	Name	Description
	Show Help	Displays help.
	Exit	Exits Configuration Browser.

Right Toolbar Buttons

The right toolbar contains the following buttons:

Configuration Browser right toolbar buttons		
Icon	Name	Description
	Add	Adds a configuration item.
	Edit	Edits the selected item.
	Delete	Deletes the selected item.
	Rename	Renames the selected item.
	Find	Initiates a search for items or values.
	Refresh	Updates the selected part of the configuration and undoes unsaved changes.
	Apply	Commits changes made in the configuration.
	Export	Exports configuration data as an .xml file.
	Import	Imports configuration data from the selected .xml file.

Setting Up Folder History Browsing

The folder history browsing feature is used to navigate between related folders.

For example, a customer's current telephone bill is stored in an Exigen Workflow folder. Using folder history browsing, an authorized Exigen Workflow user can open the folder with the current bill and navigate from it to other folders containing the customer's previous bills.

If configured, the folder history browsing feature is available in the Retrieve node and the **Folder Snapshot** window in the Queue node.

The following conditions must be fulfilled to use folder history browsing:

- The folder numbering system must be set up to ensure that previous folders can be identified. For example, if each folder contains a customer insurance policy, each folder is assigned an A_POLICY_NUMBER value, which identifies the current policy, and an A_PREVIOUS value, which identifies the previous policy.
- Folder history browsing must be configured in Configuration Browser.

Before setting up the folder history browsing feature, ensure that the Exigen Workflow database is updated. For information on updating the database, see the *Exigen Workflow Installation Guide*, Chapter 2: Installing Exigen Workflow, Creating or Upgrading the Exigen Workflow Database Structure.

This section describes the following procedures to set up the ability to browse the folder history:

- [Creating a Link Navigation Section](#)
- [Specifying Link Navigation Settings](#)

Creating a Link Navigation Section

To create a link navigation section, proceed as follows:

1. Start Configuration Browser as described in [Starting Configuration Browser](#).

The **Set Filter** window appears.

2. In the **Set Filter** window, ensure that **Configuration** is selected.
3. Click **OK**.
5. To add a new configuration section, select **Edit > Add Section**.

The **New Section** window appears.

6. To open the predefined configuration section for browsing the folder history, in the **Name** field, enter *LinkNavigation*.
7. To specify the workflow in which browsing the folder history is enabled, enter a number in the **Workflow ID** field.

The **Name** and **Workflow ID** fields must contain values. The other fields must remain empty.

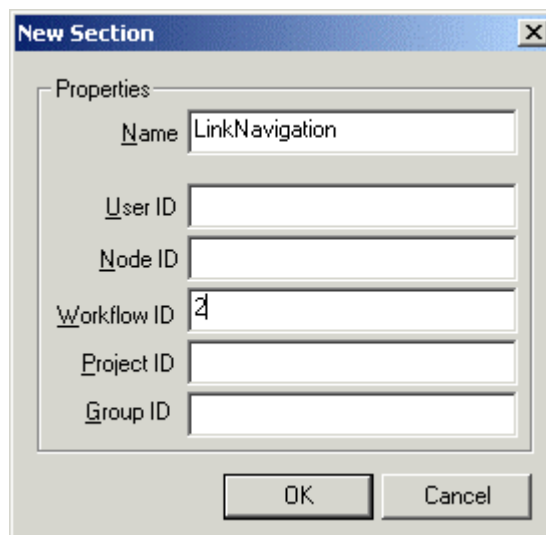
The image shows a 'New Section' dialog box with a title bar containing a close button. Inside, there's a 'Properties' section with several text input fields. The 'Name' field is filled with 'LinkNavigation'. The 'Workflow ID' field is filled with '2'. The other fields ('User ID', 'Node ID', 'Project ID', 'Group ID') are empty. At the bottom, there are 'OK' and 'Cancel' buttons.

Figure 163: Creating a link navigation section

8. Click **OK**.

The **Link Navigation** section appears in the right pane.

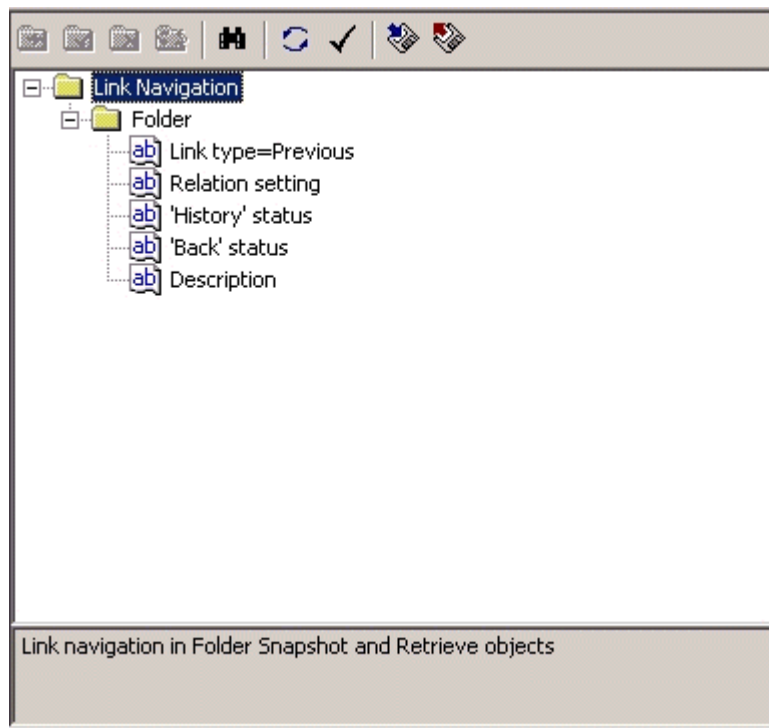


Figure 164: New link navigation section

Specifying Link Navigation Settings

To specify link navigation settings, proceed as follows:

1. To specify the relation setting, right-click **Relation setting** and select **Edit**.

The **Relation setting** item must contain a statement describing how the current folder relates to the previous folder.

2. In the **Relation setting** field, enter appropriate values.

For example, the following is entered:

```
A_POLICY_NUMBER=@A_PREVIOUS
```

3. To save the new value, press **ENTER** or click **Apply**.

By default, the **Link type** item is set to *Previous* and cannot be changed. This ensures that navigation to a previous folder is specified.

Optionally, a value can be specified for the **'History' status** item to ensure that a ToolTip appears for the **History** button, which is used to retrieve previous folders.

4. To specify the **History** button ToolTip name, right-click **'History' status** and select **Edit**.
5. Enter a ToolTip name.

For example, *Previous Folder* is entered.

6. To save the new value, press **ENTER** or click **Apply**.

Optionally, a value can be specified for the **'Back' status** item to ensure that a ToolTip appears for the **Back** button, which is used to revert to the previously displayed view.

7. To specify the ToolTip name for the **Back** button, right-click **'Back' status** and select **Edit**.
8. Enter a ToolTip name.

For example, *Back to Previous View* is entered.

9. To save the new value, press **ENTER** or click **Apply**.

Optionally, a value can be specified for the **Description** item. The value is a template for the SQL statement used to retrieve the previous folder.

10. To define a SQL statement template, right-click **Description** and select **Edit**.
11. Enter a SQL statement template.

For example, the following is entered:

```
select FLD_RSN from XXX_FOLDER where SQLwhere and FLD_SEC_RSN >=0
```

12. Click **Apply**.

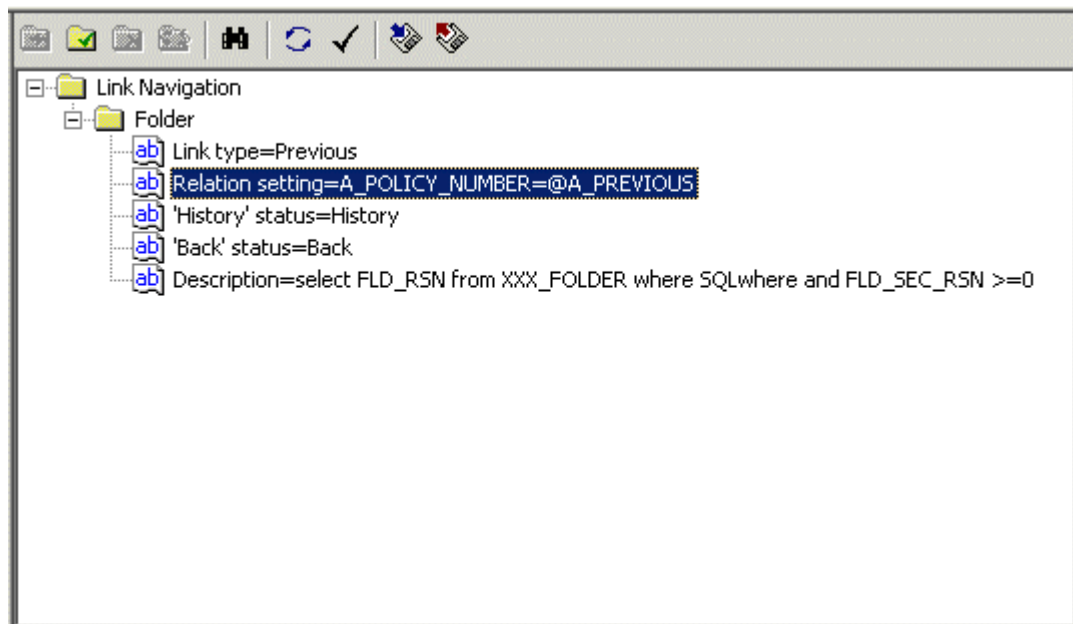


Figure 165: Completing the link navigation configuration

13. To close Configuration Browser, select **File > Exit**.

For information on using the browsing folder history feature, see the *Exigen Workflow User's Guide*, Chapter 7: Queue Processing, Folder Snapshot Window.

Specifying Scanner Specific Settings

Scanner specific settings can be configured by clicking the setup button in the scan window settings tab. After settings are changed, the user is prompted for the configuration name. When a scanner configuration is saved, it can be selected in the **Scan** window, in the **Settings** tab, from the **Scan settings** combo box.

By default, the configuration is available only to the user who created the configuration. To allow all users to access a configuration, the scanner settings file must be manually edited by changing a user in the configuration section name to COMMON. For example, if a user DTM saves a configuration named LIGHT, to allow all users to access LIGHT, in the `kofax.ini` file, the section [DTM: LIGHT] must be renamed to [COMMON: LIGHT].

To distinguish between common and user configurations, the common configurations are prefixed with the * symbol in the **Scan** window, in the **Settings** tab. Configuration files are located in the `Windows` folder.

The following is an example of a `kofax.ini` configuration file for the Kofax scanner:

```
[DATAMAX SCAN SETTINGS]
ImgControls=Version 3.XX
[DTM: CURRENT]
IOStgFlt=TIFF
IOCompression=8
Display=-1
[COMMON: Test]
IOStgFlt=TIFF
IOCompression=8
Display=-1
```

The preceding example shows a configuration for the user CURRENT, and a global configuration, Test, that is available to all users.

Chapter 5: Designing a Workflow

This chapter describes how to create and implement a workflow using Workflow Builder. The following topics are described in this section:

- [Overview](#)
- [Designing a Workflow Map](#)
- [Using Workflow Builder](#)
- [Setting Up Workflow Objects](#)
- [Setting Up Workflow Links](#)
- [Modifying Workflows in List Mode](#)
- [Using an Alias](#)
- [Using a Case](#)
- [Creating a Submap](#)
- [Setting Up Workflow Routing Rules](#)
- [Integrating with Exigen E-Forms](#)
- [Using an Oracle Stored Procedure for the Common Queue](#)
- [Simulating a Workflow](#)
- [Using Designer Mode](#)
- [Using the Hidden Mode Feature](#)
- [Setting Viewer Focus](#)
- [Tips for Building a Workflow](#)
- [Exporting and Importing a Workflow](#)
- [Managing Components](#)

Overview

A **workflow** is a graphical representation of the flow of documents, procedures, and tasks in your organization or department. A workflow provides the tools to manage, organize, distribute and archive documents and associated information needed to successfully complete the document management process. The document management process manages electronic images of paper documents and computer-generated material.

Using a workflow, you can organize the daily routing of documents from one operation process to another and from desk to desk.

A workflow must be linked to an existing project in order to know what kind of documents it is processing. However, one project can have several workflows assigned to it. Once a workflow is


created, regular users can see it as an application in the **Applications** folder in Exigen Workflow Explorer.

The following topics are described in this section:

- [Main Concepts](#)
- [List of Workflow Objects](#)
- [Main Steps to Creating a Workflow](#)

Main Concepts

Before you build a workflow for your project, you must be familiar with general workflow concepts. A workflow is the structure of how documents are processed in your business or department. It defines the procedures that occur after a document is received. The two basic components of a workflow are the **workflow objects** and **workflow links**.

Workflow concepts	
Name	Description
Workflow object	<p>Node on a workflow map that represents a specific document process such as scanning, indexing, reviewing, or archiving. Each workflow object must have a unique name that signifies its function. Some examples are <i>Clair's Scanning Station</i> or <i>Invoice Processing</i>.</p> <div data-bbox="662 940 1198 1098"></div> <p>A workflow object represents a process and location where users perform their day-to-day duties, such as sending a letter to a customer when they receive a specific document. Exigen Workflow supports six classes of workflow objects:</p> <ul style="list-style-type: none">• Scan• Index• Inspect• Queue• Archive• Miscellaneous <p>Each class is designed to perform different functions within the workflow.</p>
Workflow links	<p>Links that connect workflow objects and control the flow of documents through the workflow. When you add a link, you are defining to which target node a source node can send documents. In doing so, you are ensuring that the documents are routed and processed properly. Links can be one-way or two-way.</p>
Workflow map	<p>Graphical representation of the flow of documents, procedures, and tasks within your organization or department. The system administrator defines and builds a workflow using workflow objects and links by placing them on a workflow map.</p>
Submap	<p>Section of a workflow represented by a single icon on the main workflow map. This icon opens a new workflow map window. Links from the nodes on the main map to the icons on the submap represent the logical flow of documents to the nodes in the submap. Exigen Workflow uses submaps to simplify a workflow map.</p>

The following example shows a simple workflow containing 5 workflow objects with logical business practice links between them. The missing link for the Retrieve object is described later in this guide.

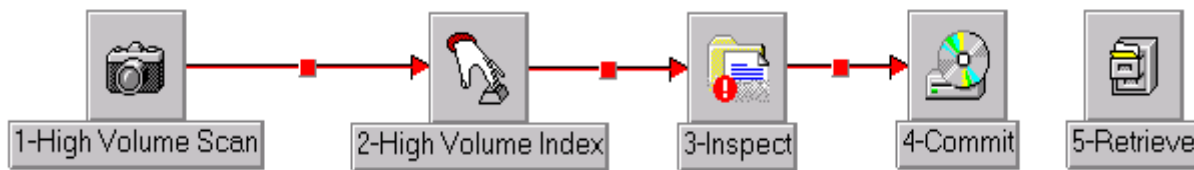








Figure 166: Simple workflow map















To accommodate all processes in your business, the workflow map can become quite large and confusing. Linking objects on the map adds to the confusion. Submaps simplify a workflow map.


List of Workflow Objects

The administrator must recognize Exigen Workflow objects when building workflow maps.

The workflow objects available in Exigen Workflow are as follows:

Workflow objects		
Object	Button	Description
High Volume Scan		Uses a scanner to convert paper documents into computer images. Multiple pages are scanned into the system as a batch, which can be separated into individual documents. In contrast to Low Volume Scan, which scans and indexes documents, High Volume Scan is used for scanning only.
High Volume Index		Assigns each scanned document to a folder or subfolder. This process joins related documents into subfolders and related subfolders into folders. Exigen Workflow automatically assigns a unique ID to each document.
Low Volume Scan		Combines the operations of High Volume Scanning and High Volume Indexing and applies them to small quantities of documents.
Inspect		<p>Quality assurance process. Inspection determines whether a scanned image meets quality standards or if it must be re-scanned or repaired. Exigen Workflow automatically indicates that a document must be inspected if at least one of the following occurs:</p> <ul style="list-style-type: none"> A page of the document is larger or smaller than the size specified in the system attributes by the system administrator. The document is the n^{th} document, and every n^{th} document is inspected. The system administrator assigns the value for the n^{th} constant.
Queue		Allows users to include a word processor, spreadsheet, or other external application in the workflow process. The tasks performed with the document images are part of the regular day-to-day duties and are performed in the Queue workflow object.
Retrieve		Allows users to retrieve folders or documents for browsing, editing, or printing. Full Text Search retrieval can be used to search for specific words or phrases within the pages of the documents.

Workflow objects		
Object	Button	Description
Work Item Submitter		Has all the functionality of the Retrieve object and creates parcels from retrieved documents that can be sent to the next workflow node.
Barcode Server		Reads bar codes in documents being scanned. The server converts the values into commands that create parcels for the documents and populate the document index fields.
Commit		Sends documents to a predefined storage medium, usually an optical disk. The Commit configuration specifies the location and size of the storage media as well as the documents to be stored.
Distribution Server		Exports images and their corresponding database information from one database to another.
Escalation Server		Routes work items and email to users defined in those queues in the workflow that are escalation-enabled.
ERM Indexer		Extracts data from text files according to a specified model and fills Exigen Workflow tables with the extracted data. This information can be used in Enterprise Report Management (ERM) and Forms Overlay processing.
ERM Setup		Registers the text files, models, and templates that are processed into ERM, Form Overlay, or COLD format via the ERM Indexer.
ERM Storage Maintenance		Moves ERM storage files from the original location to any other location on the network, including optical storage.
FTS (Full Text Search) Preprocessor		Extracts text from each page of every document sent through the workflow. It performs Optical Character Recognition (OCR) on images and uses other methods for other file formats, including DOC, PPT, XLS, and PDF. Custom Conversion Engine plugins can be developed for specific formats. Document search and retrieval can be performed based on the document text.
FTS Server		Creates the FTS Index, which is used to search for documents based on text values.
Form Index Server		Populates the database with data extracted during the Form OCR process.
Form OCR QA		Checks and corrects the data extracted during the Form OCR process.
Form OCR Server		Extracts OCR data from incoming documents based on templates.
Image Enhancement Server		Improves the quality of scanned images. The same enhancements are available during the scanning process; however, the number of enhancements configured in the scanning process directly corresponds to the amount of time it takes to perform the scanning. Using the server decreases scanning time while ensuring image integrity.

Workflow objects		
Object	Button	Description
Import Server		Can import documents into the Exigen Workflow repository without scanning and index the imported documents. The imported documents can be in different formats, including Exigen Workflow DMS, DOC, PDF, HTML, GIF, and JPEG.

Main Steps to Creating a Workflow

To create a workflow, proceed as follows:

1. Design it manually.

Attempting to create an electronic workflow without first documenting and reviewing all the steps is difficult, and the finished product may not adequately represent all procedures and rules associated with paper processing. Create the workflow map using the Workflow Builder application.

Building the workflow map consists of placing workflow objects on the map and adding links to simulate the flow of documents.

2. Add rules to automate document routing from one queue to another based on document field values.
3. Test the workflow.

This is done using the Simulation feature available in the Workflow Builder. It allows you to simulate actual document processing without having to log out of the workflow.

Note: Users cannot use the actual workflow while it is open in the Workflow Builder.

Designing a Workflow Map

The first step in creating a workflow is planning the map design. The next step is to define workflow objects and link them to one another to create a smooth flow of information.

If you design the workflow on paper before you create it, you save time and effort. Even though you may change the design later, careful planning reduces the total time and effort required.

Designing a workflow involves the following basic steps:

1. Decide what categories or departments of information you want to include in the workflow map and create a different workflow map for each major category. Look at the different processes you intend to automate and decide whether they are to be integrated or remain separate. This determines if you need several workflow applications or just one with multiple submaps.
2. Analyze your current flow of information to determine what processes and tasks your company currently performs. Noting mandatory approvals or responses to incoming documents assists you in creating links and routing rules. Processes include scanning, indexing, and inspecting. Tasks include letters, notes attached to documents, and reports.

3. Determine if new processes must be implemented. Exigen Workflow offers many workflow objects that replace manual processes and expedite the flow of documents. Determine where in the workflow these processes suit your business practice.
4. Analyze the volume of documents processed through the workflow to determine how many separate desktops or workflow objects are required to perform each operation.
5. Estimate how long each item of information takes to process at each desktop or workflow object.
6. Organize the workflow objects in an easy-to-read flow. Each workflow object has links attached to it, and the links can be intertwined and very confusing. Mapping out the links on paper assists in the creation and interpretation of complex workflow maps.
7. Decide whether submaps are required. If a section of the workflow map is too complex, it is best to separate it into a submap.

Using Workflow Builder

The **Workflow Builder** tool customizes all aspects of a workflow. As part of this process, you can perform the following tasks:

- quickly change the routing of documents
- add or change user groups assigned to a workflow object
- view graphic maps of the workflow process
- track all jobs and their locations in the workflow

The **Workflow Builder** is located in the **Workflow Tools** folder in **Administration Tools** in Exigen Workflow Explorer.

If Taskflow Server is installed, it is possible to specify one of the following workflow types when creating a workflow:

Workflow types	
Type	Description
Workflow	Standard workflow. A standard workflow consists of nodes connected by links.
Taskflow	Workflow for Task Oriented Workflow. For information on taskflows, see the <i>Task Oriented Workflow Administrator's Guide</i> .
Tasklist	List of tasks for Task Oriented Workflow. For information on tasklists, see the <i>Task Oriented Workflow Administrator's Guide</i> .
Processflow	Process workflow. A processflow is a set of process steps connected by links. For information on processflows, see the <i>Task Oriented Workflow Administrator's Guide</i> .

Note: The ability to distinguish between workflow types is not available in standard Exigen Workflow client/server and Web applications. It is supported by programmable extensions only, and is available via application programming interfaces (APIs). For information on how to acquire this feature, contact Exigen Support Services.

To create a taskflow, tasklist, or processflow, follow the instructions as described in the *Task Oriented Workflow Administrator's Guide*.

To create a standard workflow, proceed as follows:

1. To open the **Workflow Builder** window, click the **Workflow Builder** icon.



The **Workflow Builder** window appears.

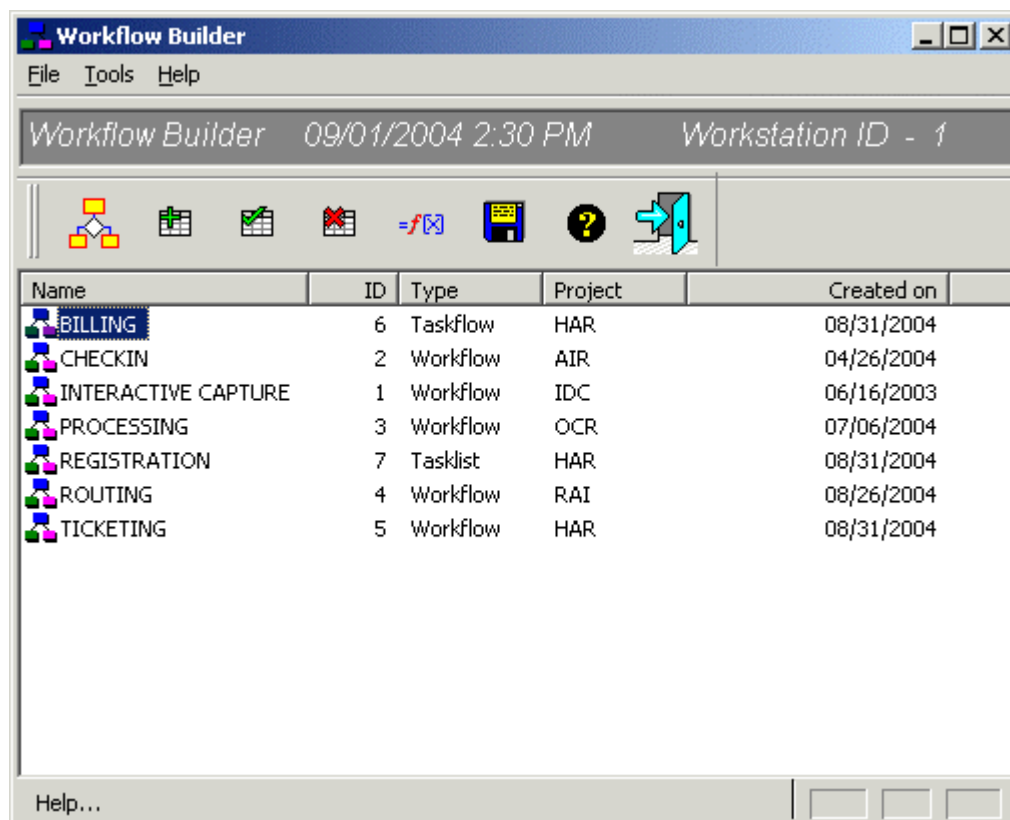


Figure 167: Workflow Builder window

The table lists all workflows that exist in the system.

The **Type** column appears only if Workflow Builder is set up to distinguish between workflow types.

2. Click **New**.



The **Create New Workflow** window appears.

Figure 168: Create New Workflow window

3. In the **Title** field, enter the name for the workflow.
4. In the **Project** list, select the project to which you are attaching the new workflow.

The window displays the date and the author of the workflow.

5. To create a standard workflow, ensure that **Workflow** appears in the **Type** list.

The **Type** list appears only if Workflow Builder is set up to distinguish between workflow types.

6. To create the workflow record and return to the main **Workflow Builder** window, click **Apply**.

7. To build the workflow, select the workflow in the list and click **Builder** .

The **Workflow Map** window appears, displaying the workflow name in the title.

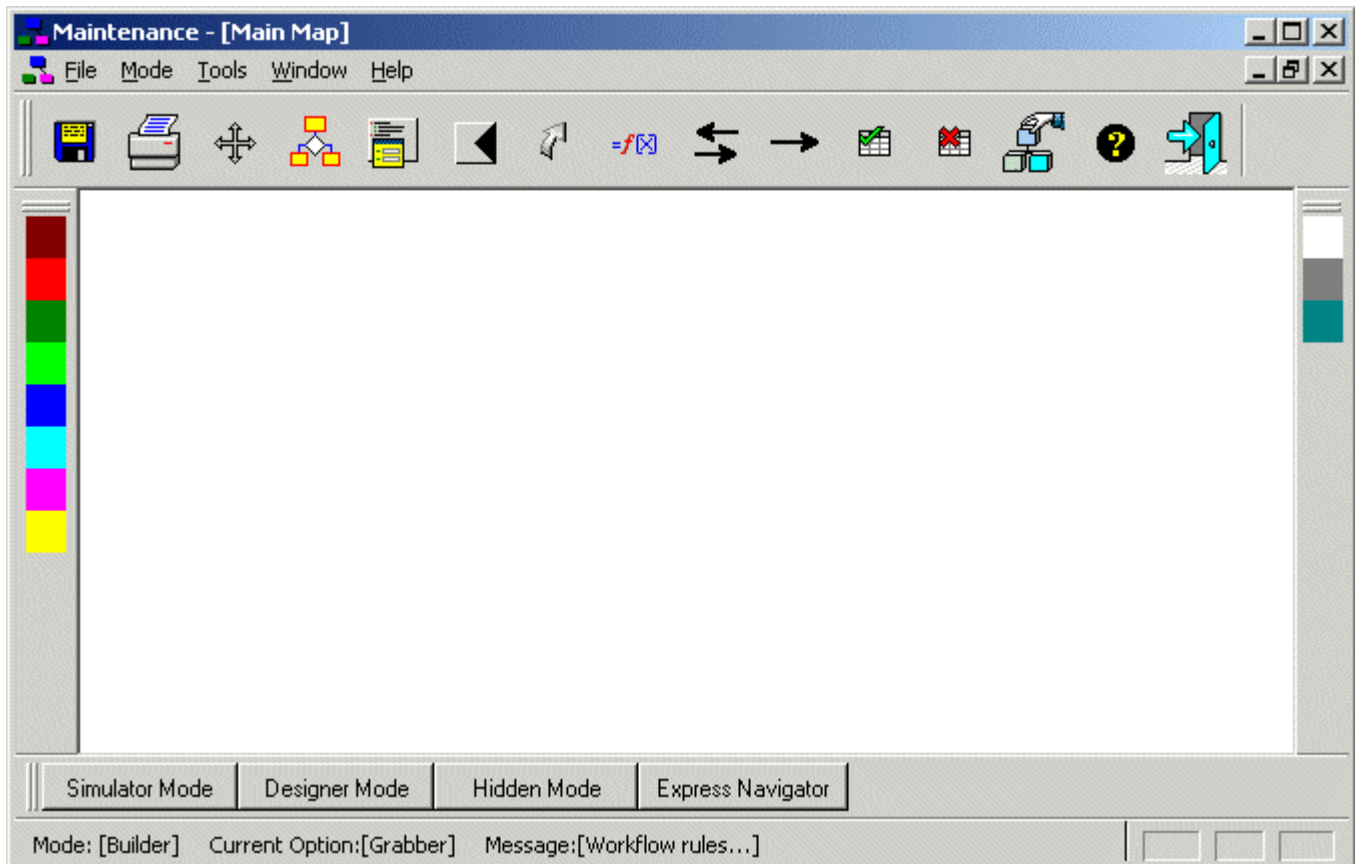


Figure 169: Workflow Map window

8. In the background color palette, select an appropriate background color for the workflow map:



If no background color is selected, the background is white.


9. To set up workflow objects, proceed as described in [Setting Up Workflow Objects](#).
10. To set up links, proceed as described in [Setting Up Workflow Links](#).

11. To configure reusable nodes, plugins, applications, and workflows in the project, click .

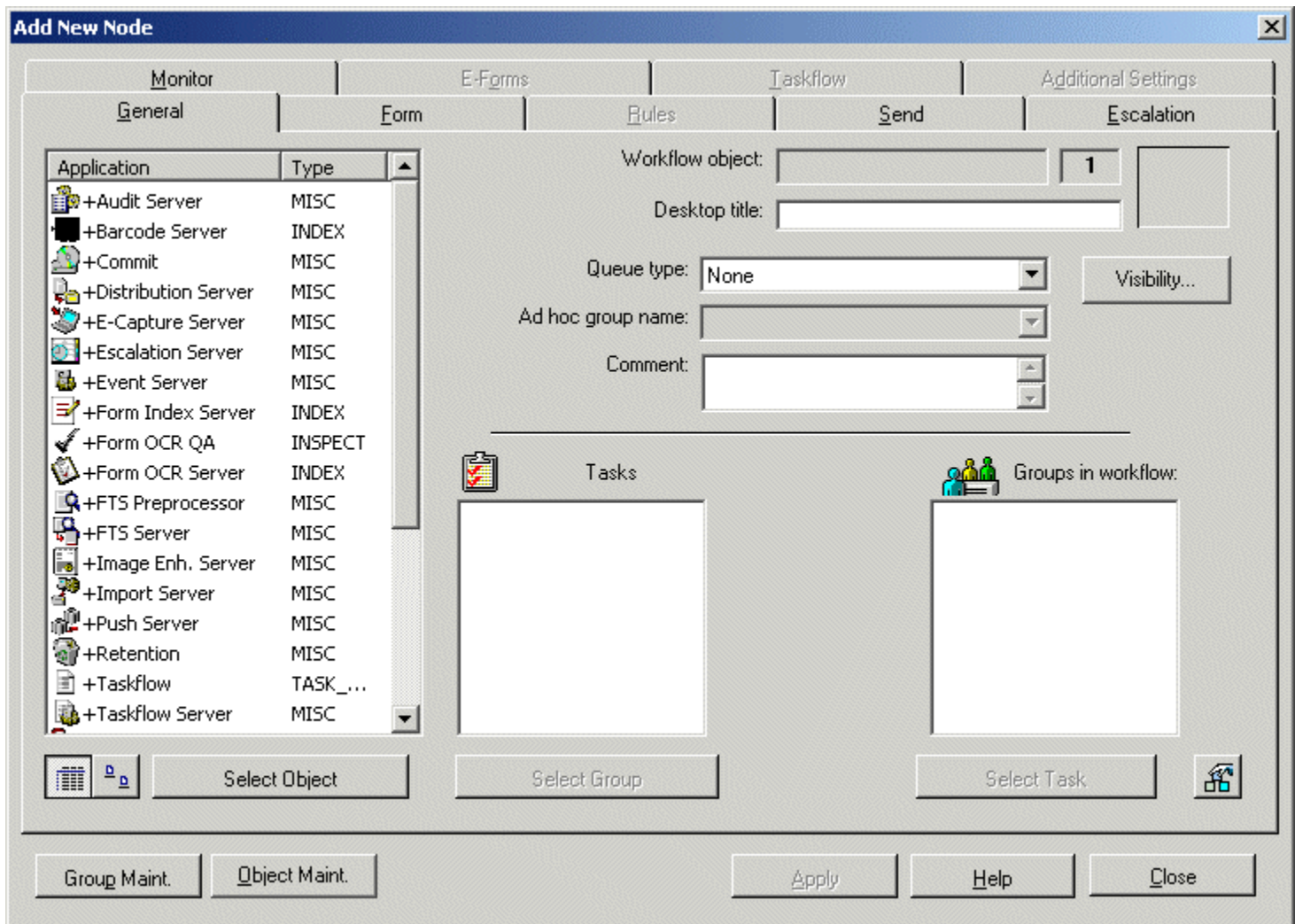
The **Component Configuration Manager** window appears. For information on Component Configuration Manager, see [Managing Components](#).

Setting Up Workflow Objects

To add a workflow object, proceed as follows:

1. Click the **Node Creation** tool .
2. Select a location for the node and click it.

The **Add New Node** window appears.



The **Add New Node** window is shown with the following components:

- Tabs:** Monitor, E-Forms, Taskflow, Additional Settings.
- Sub-tabs (under Monitor):** General, Form, Rules, Send, Escalation.
- Left Panel (Application List):**

Application	Type
+Audit Server	MISC
+Barcode Server	INDEX
+Commit	MISC
+Distribution Server	MISC
+E-Capture Server	MISC
+Escalation Server	MISC
+Event Server	MISC
+Form Index Server	INDEX
+Form OCR QA	INSPECT
+Form OCR Server	INDEX
+FTS Preprocessor	MISC
+FTS Server	MISC
+Image Enh. Server	MISC
+Import Server	MISC
+Push Server	MISC
+Retention	MISC
+Taskflow	TASK_...
+Taskflow Server	MISC
- Right Panel (Configuration):**
 - Workflow object:
 - Desktop title:
 - Queue type:
 - Ad hoc group name:
 - Comment:
 - Buttons: Visibility...
- Bottom Section:**
 - Tasks:
 - Groups in workflow:
 - Buttons: Select Object, Select Group, Select Task, Group Maint., Object Maint., Apply, Help, Close.

Figure 170: Add New Node window

General Tab

The **General** tab shows an object list displaying all workflow objects registered in your project.

To specify settings in the **General** tab, proceed as follows:

1. To select an object, select it and click **Select Object**, or double click it.

The **Workflow object** field on the right shows the selected object's name and the internal node ID. When parcels and documents move from queue to queue, the internal node ID field in the respective tables reflects this value.

The **Desktop title** by default is the same name as a workflow object's name.

2. Change the desktop title as appropriate.

Users see the desktop title at their workstations, so it must be meaningful to them. Note that the node ID precedes the name when the node is added to the workflow.


Each node is defined as a certain type. The type appears in the **Queue type** field. Each type is used to identify special actions to be performed or allowed by the node. The four node types are described in the following table:

Node types	
Type	Description
None	No special attributes are assigned to the node.
Pending	Parcels assigned to the same folder are merged with the parcel that already exists in the node. The same folder is assigned when received in this node.
Rendezvous	Parallel parcels are merged when received in this node.
Ad hoc	<p>Nodes of this type can send a parcel to each other without workflow links. An Ad hoc node can also send parcels to itself.</p> <p>If the node is defined as an Ad hoc node, you can assign Ad hoc groups to work with the node. If there are no Ad hoc nodes, enter a name in the Ad hoc group name field. Exigen Workflow remembers this group name, which you can select in the list of any other Ad hoc nodes. This node type only allows an Ad hoc node with the same Ad hoc group name to send a parcel to similar nodes. For example, Ad hoc node group A can only send a parcel to Ad hoc node group A, but not to Ad hoc node group B. If no Ad hoc groups are required, leave this field blank.</p>

A node that has an Ad hoc type is identified by a yellow marker in the lower-left corner of the icon.



Figure 171: Ad hoc node

3. To configure node extended attributes and associations with plugins and applications, click .
4. Component Configuration Manager is opened for the node. For information on Component Configuration Manager, see [Managing Components](#).
5. To configure the node visibility settings, click **Visibility**.

The **Node Visibility** window appears.

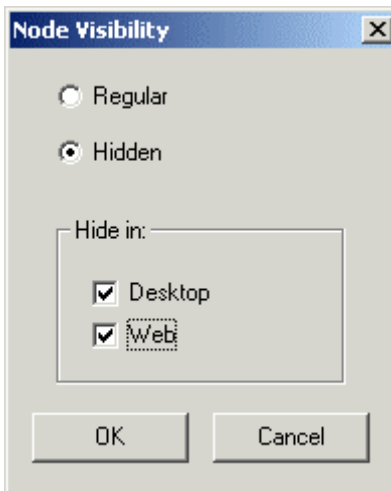


Figure 172: Node Visibility window

6. In the **Node Visibility** window, select one of the following options:
- To make the node visible to all users who have access to the node, select **Regular**.
This is the default option.
 - To hide the node from users, select **Hidden** and, in the **Hide in** section, select the following options as required:

Hiding options	
Option	Description
Desktop	Hides the node in Exigen Workflow Explorer.
Web	Hides the node in the applications list and To Do list in Exigen Workflow Web.

Typically, hidden nodes are system nodes that do not require direct user interaction. Hidden nodes are visible in Workflow Builder, Workflow Viewer, and Workflow Monitor. No security restrictions apply to hidden nodes, and documents located in hidden nodes can still be retrieved using Retrieve and Work Item Submitter.

7. In the **Comment** field, enter a description of the node.
8. To change users in each group, click **Group Maint.**

The **Groups for selection** list defines workflow groups that can use the node. Groups are defined in the system through the System Setup function in the **Administrator Utilities** window. For more information on groups, see [Chapter 4: Setting Up Exigen Workflow](#).



Figure 173: Adding groups to a node

9. To assign groups, click **Select Group**.

All groups in the system are listed on the left. Assigned groups are listed on the right.

10. To arrange groups that use the node, click the appropriate buttons.
11. To apply the groups, click **OK**.

Tasks can be assigned to each node. A task must be set up before assigning it to a node. For more information on setting up tasks, see [Setting Up Tasks](#).

Tasks can be assigned to all nodes, but restrictions on task actions apply as described in [Restrictions on Task Actions in Nodes](#).

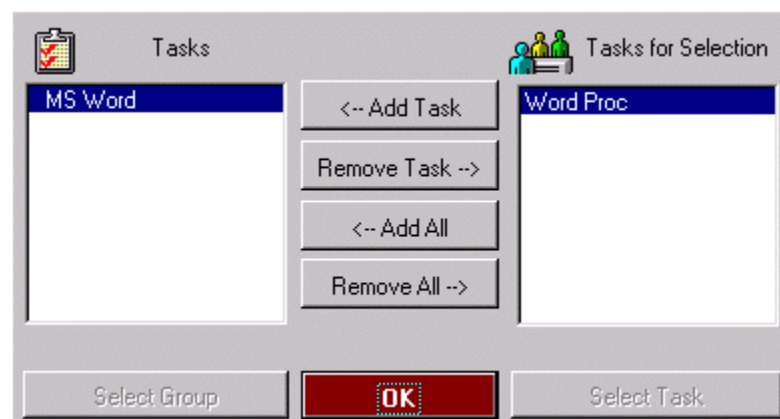


Figure 174: Adding tasks to a node

12. To assign tasks, click **Select Task**.

All tasks in the system are listed on the right.

Assigned tasks are listed on the left.

13. To arrange tasks performed by this node, click the appropriate buttons.
14. To define an assigned task as mandatory, in the **Tasks** list, double click the task.

The task is marked with a circumflex symbol.

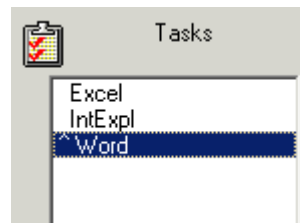


Figure 175: Specifying a mandatory task

If a task is specified as mandatory, it must be performed before the parcel can be sent to the next node.

15. To apply the tasks, click **OK**.

16. To change the default icon for the node, in the lower left part of the **Add New Node** window, click **Icon**.

The assigned icon appears to users in Exigen Workflow Explorer.

17. To modify workflow objects, click **Object Maint.**

The **Object Maint.** button is not available if the user does not have the administrator rights.

The **Workflow Object Setup** window appears. For information on using the **Workflow Object Setup** window, see [Setting Up Workflow Objects](#).

Restrictions on Task Actions in Nodes

Depending on the node's workflow object type, restrictions can apply to task actions performed in nodes.

The following workflow objects can run task applications and create task documents:

- Inspect
- Queue
- High Volume Index
- Low Volume Scan

The following workflow objects can only run task applications for which the **Launch Task (No Document is Created)** option is selected, and do not create task documents:

- Retrieve
- High Volume Scan
- Work Item Submitter

For more information on tasks, see [Setting Up Tasks](#).

Form Tab

The **Form** tab assigns **form executables** or other outside applications to the node.

Modify Node

Monitor | **E-Forms** | Taskflow | Additional Settings

General | **Form** | Rules | Send | Escalation

Workflow object:

Desktop title:

Form executable: ..

Form parameter: ..

☐ Auto load

☐ Enable stored procedure

Stored procedure for a common queue:

Figure 176: Modifying a node, Form tab

To specify settings in the **Form** tab, proceed as follows:

1. To locate the executable in the system, click the browse button.

Note: The path to the form executable cannot exceed 60 characters.

2. To add startup parameters to the executable, specify them in the **Form parameter** field. You can also select a script file to use with the form executable.

The executable is launched when the user opens the node.

Note: The form parameter cannot exceed 60 characters.

- To ensure that the next unprocessed document in the queue automatically appears with the form, select the **Auto load** check box.

If you do not select the **Auto load** check box, the form is opened without content, and the user must select the next unprocessed document manually from the queue.

Note: If you are using an Oracle database, it is possible to apply a special stored procedure. For information on special stored procedures, see [Using an Oracle Stored Procedure for the Common Queue](#).

The Form Executable feature is especially useful for indexing purposes. For example, you can create a form that replaces the functionality of the Assign to Folder, Subfolder, and Document Type features of the Index node. This combines them into a form, which has all the fields required to index the document. This form can be launched for the selected document in the queue automatically, or by selecting the **Activate Host Session** item in the **File** menu of the node.

Note: The **Auto load** option cannot be used for the High Volume Scan node. High Volume Scan does not have host session functionality and cannot be used to index documents.

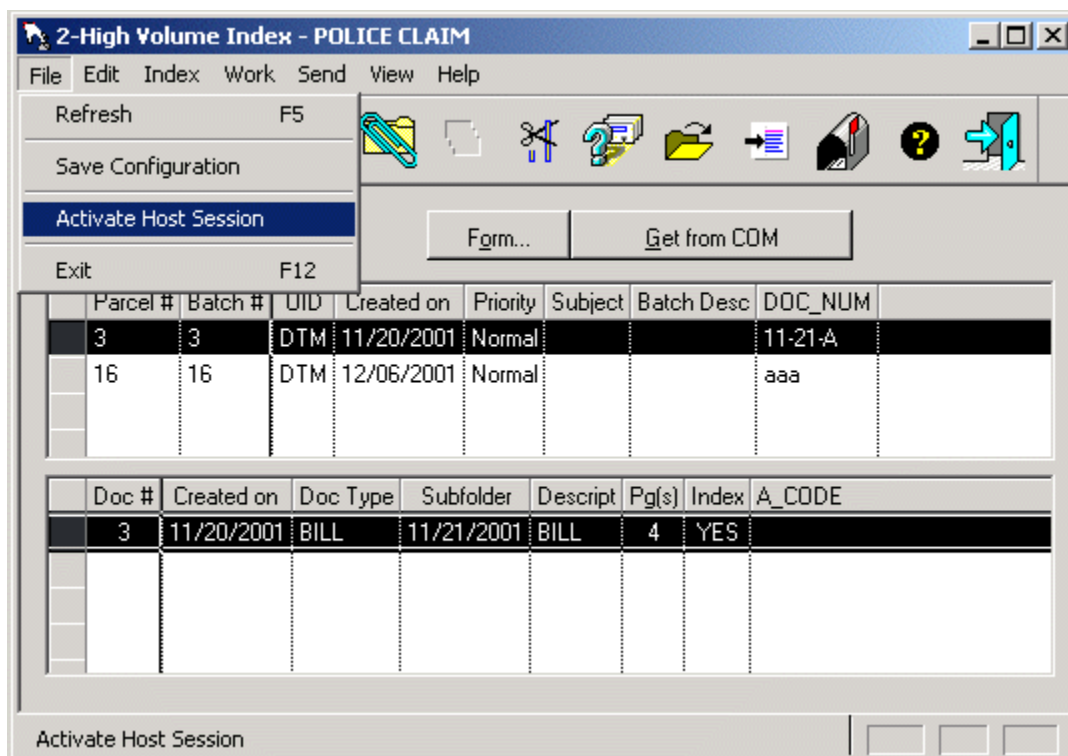


Figure 177: Launching the executable form from the node

To activate the **Auto load** option on a local computer, proceed as follows:

- In the EWF\INI directory, open the visiclt.ini file.
- In the Host Integration section, locate the node for which the **Auto load** option must be set.

The **Auto load** option can be set for the following nodes:

- High Volume Indexing
- Low Volume Scanning

- Queue
 - Inspect
 - Archive
3. Set the `auto` value to `YES` as in the following example for High Volume Indexing:

```
[host_index]
program=
script=
auto=YES
```

4. Save and close the `visiclt.ini` file.

For example, you can use the Exigen Workflow form executable `frmcomm.exe`. When you activate your host session, the **Select from the Common Queue** utility window appears. You can pull one or several parcels from the selected common queue.

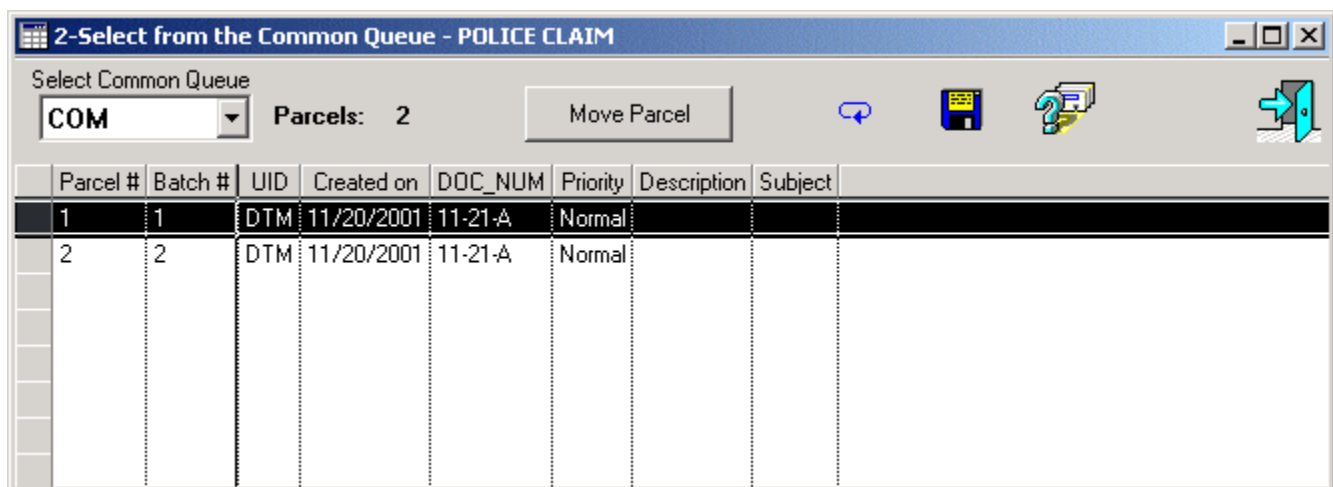


Figure 178: Select in the Common Queue utility window

All parcels in the selected common queue are shown.

To work with parcels, proceed as follows:

1. To pull a parcel to your queue, select it and click **Move Parcel**.
The parcel appears in your queue.
2. To update the parcel list in the common queue, click **Refresh**.
3. To search for a parcel, in the **Query Parcel Records** window, click **Find** and specify your query.

Note: You can launch only one Select from Common Queue utility on your workstation at a time.

You can write your own forms to use as form executables.

Rules Tab

The **Rules** tab is disabled when you are adding a new node. This tab is enabled only when you have linked nodes and want to establish routing rules that govern the flow of documents through the workflow. For information on routing rules, see [Setting Up Workflow Routing Rules](#).

Send Tab

The **Send** tab assigns basic sending options.

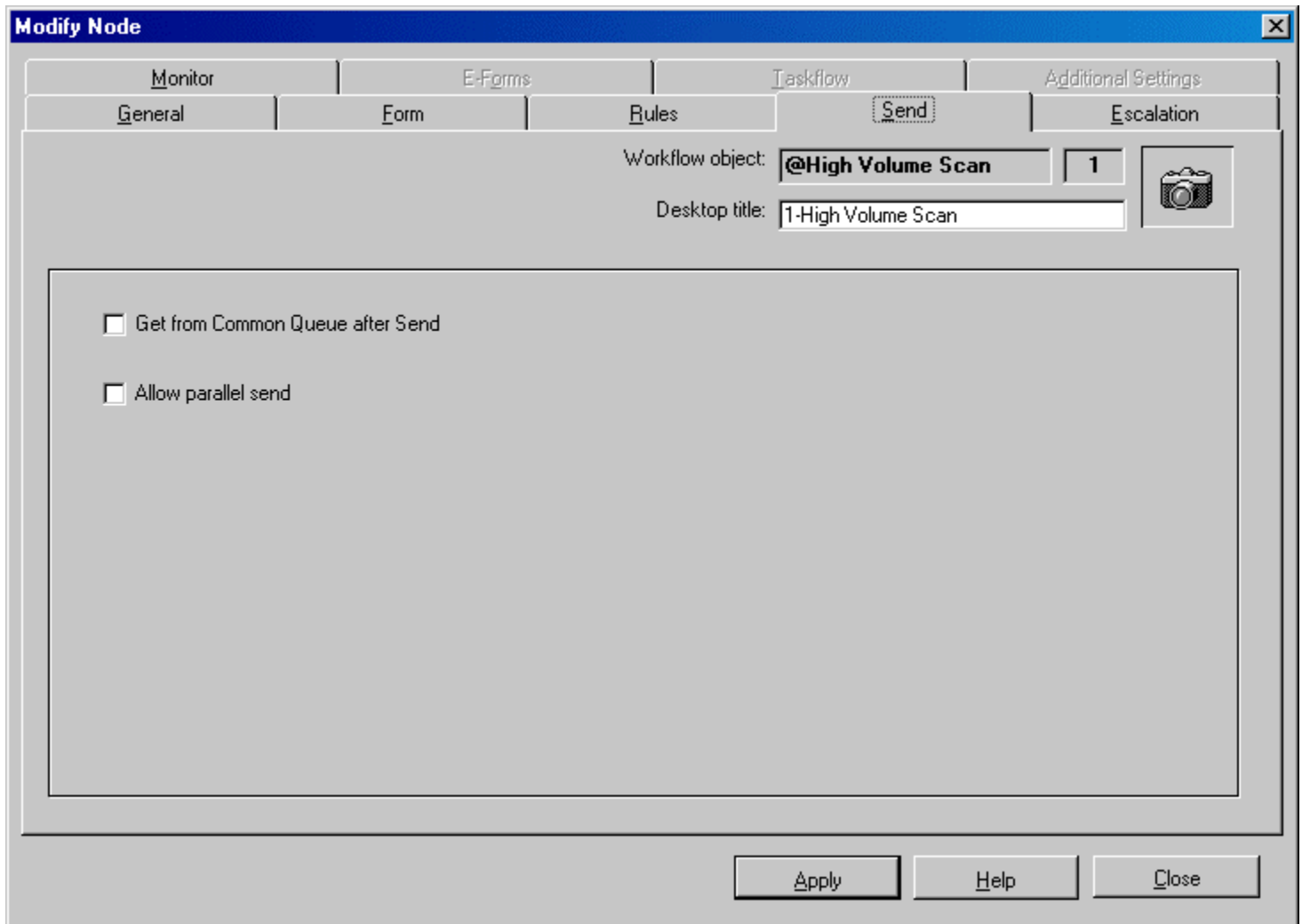


Figure 179: Modifying a node, Send tab

The **Get from Common Queue after Send** option automatically pulls the next job from the common queue.

Note: If the **Get from Common Queue after Send** option is selected in Workflow Builder, it cannot be disabled by the user's local settings.

To send a parcel to more than one queue and user, select the **Allow parallel send** check box. This feature is usually used in the Queue object. You might want to include a rendezvous queue later in the workflow to collect and combine parallel parcels.

Escalation Tab

The **Escalation** tab is used to place time restrictions on how long jobs can remain in a specific node. A time period in days, hours, or minutes can be assigned to the node. Once a job has expired, it is sent to a designated queue and user. You can assign events to occur during the escalation process, and notify additional users via email about the parcels that have expired.

Modify Node

Monitor | E-Forms | Taskflow | Additional Settings

General | Form | Rules | Send | **Escalation**

☒ Enable Escalation

Workflow object: @High Volume Scan 1

Desktop title: 1-High Volume Scan

Execute after: 1 Days Time period: ☒ Days ☐ Hours ☐ Minutes

Send to queue: 10-Commit Clear the Queue and User

Send to user: DTM

Routing description:

Email to:

Mail profile:

Events to execute:

Event Name	Prt	Event Parameter String
Audit log housekeeping	1	12345678901234567890123456789012345

Add... Modify... Delete

Apply Help Close

Figure 180: Modifying a node, Escalation tab

To specify settings in the **Escalation** tab, proceed as follows:

1. To use the escalation function in the current node, select the **Enable Escalation** box.
2. Note that once the **Escalation** tab is configured, clearing this box does not reset the values. If escalation is required in the future, reselect the check box.

3. In the **Execute after** field, enter the number of days, hours, or minutes to set as the threshold. Select the **Days**, **Hours**, or **Minutes** option to specify the time period.
4. In the **Send to queue** list, select the target queue for the parcels meeting the escalation criteria.
5. Note that because all queues in the current workflow are listed, the escalation source and target nodes do not have to be linked. The target node must already exist in the workflow.
6. In the **Send to user** list box, select the user you want to send the escalated parcels to.

The user list is independent of the users assigned to the selected node.

5. To remove the values from the preceding two fields, click **Clear the Queue and User**.
6. In the **Routing description** field, describe the purpose of the escalation.
7. In the **Email to** field, list Exigen Workflow user IDs for everyone who needs to be aware of a parcel escalation. Insert a comma as a delimiter between each user ID.
8. If a user is entered in this field, update the user profile with an email address.

The **Mail profile** list allows you to select which email product to use for sending email.

9. If you want an event to execute during the escalation process, click **Add** under the **Events to execute** table.
10. Enter any required parameters as described in [Setting Up Workflow Links](#).
11. To modify an existing event, click **Modify**.
12. To delete an event, click **Delete**.

For information on how to run Escalation Server, see the *Exigen Workflow Administrator's Guide, Part 2: Business Component Reference*, Chapter 11: Escalation Server and Log.

Monitor Tab

The **Monitor** tab identifies which workflow groups can view or distribute jobs to and from this queue. This feature works with the Security Levels where access to jobs in Monitor, Distribution, and Deletion is assigned. All workflow groups in the database are displayed in this window.

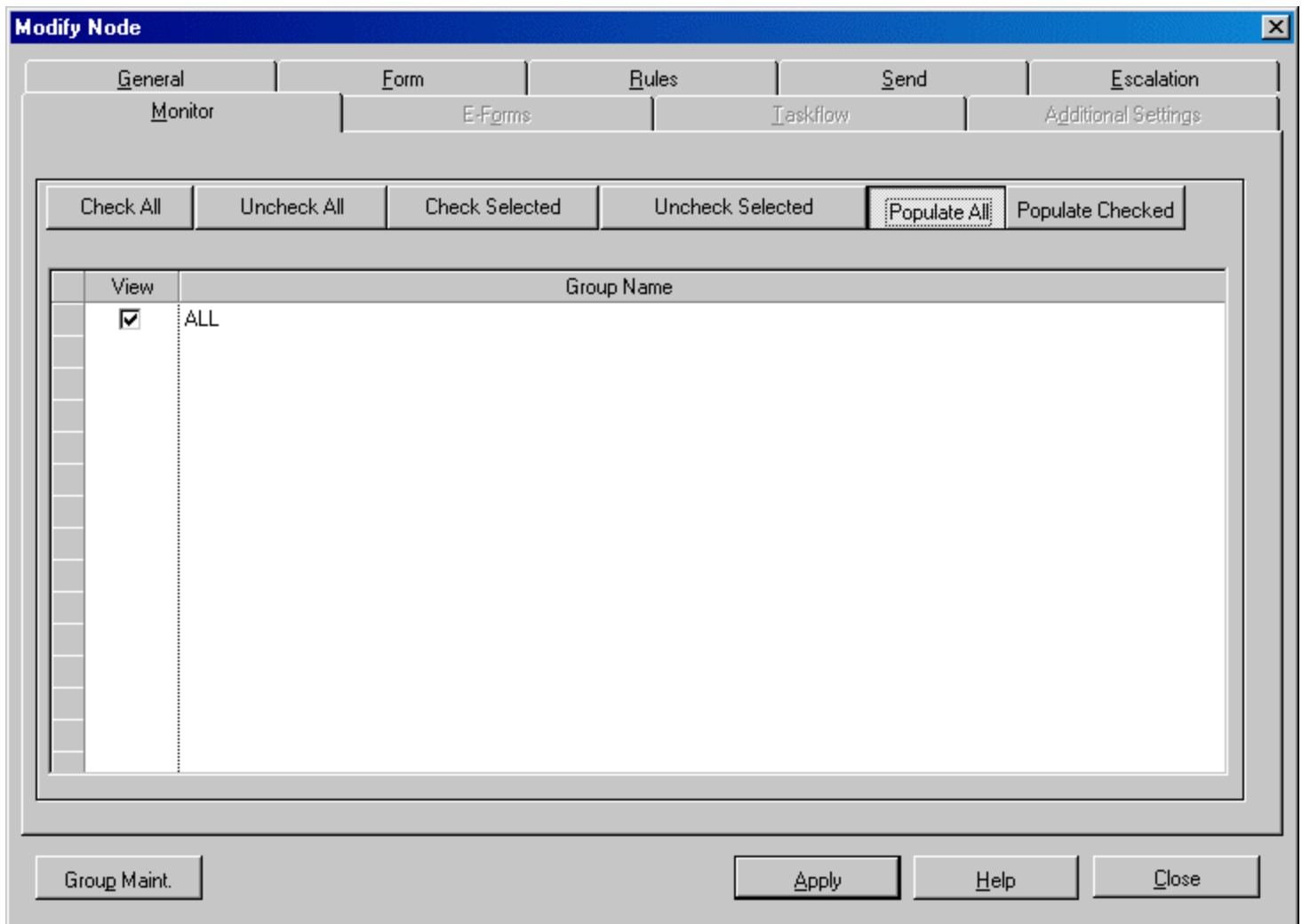


Figure 181: Modifying a node, Monitor tab

To specify settings in the **Monitor** tab, proceed as follows:

1. To allow a workflow group to access jobs in the current node, select the corresponding check box next to the group name.
2. To view all workflow groups available, click **Populate All**.
3. To limit the listing to only those groups given access, click **Populate Checked**.
4. Once all node information is complete, to add the node to the workflow map, click **Apply**.

E-Forms Tab

For information on the **E-Forms** tab, see [Integrating with Exigen E-Forms](#).

Taskflow Tab

The **Taskflow** tab is used with Task Oriented Workflow to configure task parameters in taskflows.

For more information on Task Oriented Workflow, see the *Task Oriented Workflow User's Guide* and the *Task Oriented Workflow Administrator's Guide*.

Additional Settings Tab

The **Additional Settings** tab is used for the following purposes:

- specify functions allowed in the node
- specify security handling of documents that arrive in or are generated in the node

Modify Node

General | Form | Rules | Send | Escalation

Monitor | E-Forms | Taskflow | **Additional Settings**

Workflow object: **@High Volume Scan** | 1 |

Desktop title: **1-High Volume Scan**

	Allowed	Function	Description
<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	ADD	Controls creation of new documents
<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	MODIFY	Controls modification of documents
<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	DELETE	Controls deletion of documents
<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	IMG_VIEW	Controls document image display
<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	IMG_EDIT	Controls document image editing
<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	IMG_HIDE	Controls document hidden areas creation and maintenance
<input type="checkbox"/>	<input type="checkbox"/>		
<input type="checkbox"/>	<input type="checkbox"/>		
<input type="checkbox"/>	<input type="checkbox"/>		

☒ Enable default security in this node

☒ Assign filter based security to new documents

☐ Node is server (filtering is not applied)

Apply | Help | Close

Figure 182: Modifying a node, Additional Settings tab

To specify settings in the **Additional Settings** tab, proceed as follows:

1. To specify the functions allowed in the node, in the table, in the **Allowed** column, select one or more of the following functions:

Allowed column functions	
Function	Description
ADD	Add a document.
MODIFY	Modify a document.
DELETE	Delete a document.
IMG_VIEW	View a document image.
IMG_EDIT	Edit a document image.
IMG_HIDE	Create and maintain hidden areas in a document.

Security settings can be applied to new documents in the node. New documents are those that were scanned in the node, imported into the node, or are new task documents in the Queue node.

- To specify how security settings are applied to new documents in the node, select one of the following options:

Security options	
Option	Description
Enable default security in this node	<p>ACL based security settings applied to all new documents in the node.</p> <p>Initially, all documents with defined default security are hidden from all users except in nodes where default security is enabled and except for users having grant security full permission.</p>
Assign filter based security to new documents	<p>ACL based security settings applied to new documents based on entitlements.</p> <p>The Assign filter based security to new documents option applies only if the user of the new document has grant security full or grant security limited permission.</p> <p>If both the Enable default security in this node and the Assign filter based security to new documents options are selected, and no entitlement matches a given document, the default security entry is applied.</p>
Node is server (filtering is not applied)	<p>No restrictions applied. The server has grant security full permission. All documents in the node can be accessed by the server process regardless of which user started the server.</p>

- When all node information is complete, to add the node to the workflow map or save changes in the node configuration, click **Apply**.

Maintaining Workflow Nodes

To maintain workflow nodes, proceed as follows:

- To modify a node, click the **Grabber** tool  and double click on the desired node or

click the **Modify Node/Link** tool  and click on the node.

2. Make the changes and click **Apply**.

3. To delete a node, select the **Delete Node/Link** tool  and click on the desired node.

Exigen Workflow prompts you to confirm the deletion.

Setting Up Workflow Links

Create links to connect nodes and to allow a parcel to be sent after the nodes are added to the map. Links can be one-way or two-way depending on your business needs.



To add a link, proceed as follows:

1. In the link color palette, select an appropriate link color:



If no link color is selected, the default color, red, is used.

2. Select one of the following **Link** tools:

- one-way 
- two-way 

3. Click over the source, or link from node, and drag the mouse to the target, or link to node, and release.

The **Add Link Information** window appears displaying three tabs:

- **General**
- **Events**
- **Appearance**



Figure 183: Add Link Information, General tab

The **General** tab displays the **Source** and **Target** nodes.

4. In the **Description** field, enter comments about the link.

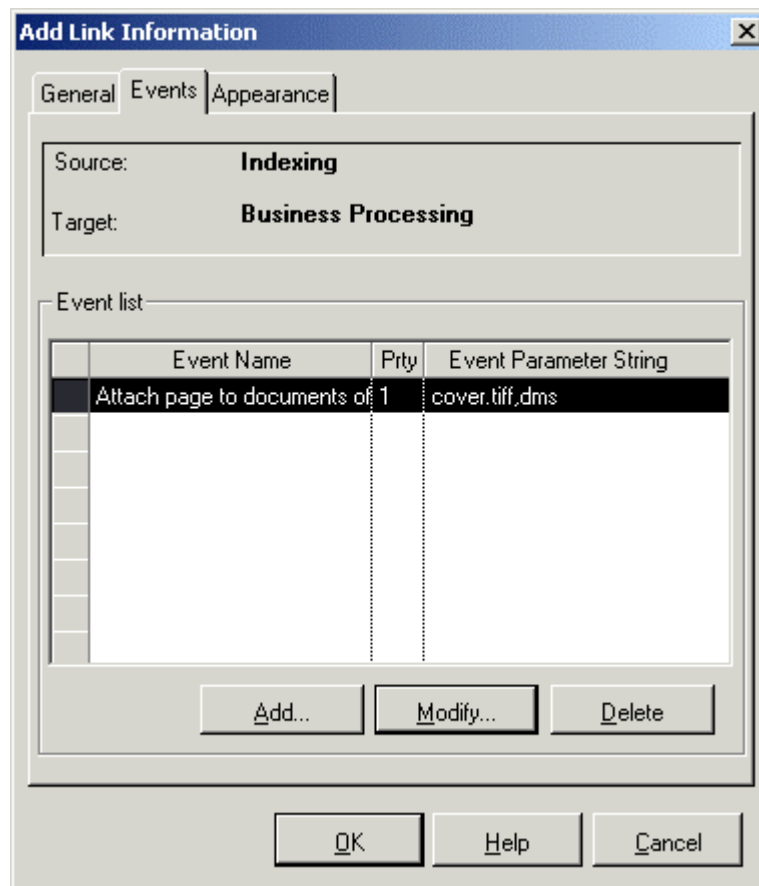


Figure 184: Add Link Information, Events tab

The **Events** tab displays the events assigned to the link. These events occur when a parcel is routed from one node to the next.

- To add a new event to this link, click **Add**.

Exigen Workflow has a number of predefined events as described in [Exigen Workflow Events](#). If you need a different event to run your business process, contact Exigen Support Services.

In the current Exigen Workflow version, Automatic Queue Server handlers are set up to process events. For more information on Exigen Workflow handlers, see the *Exigen Workflow Administrator's Guide, Part 2: Business Component Reference*, Chapter 21: Exigen Workflow Handlers.

At some customer sites, Advanced Event Server is used to process events. If Advanced Event Server is used, an Event Server node must be included in the workflow.

- To change the color of the link as well as its characteristics, the **Appearance** tab, modify the settings.

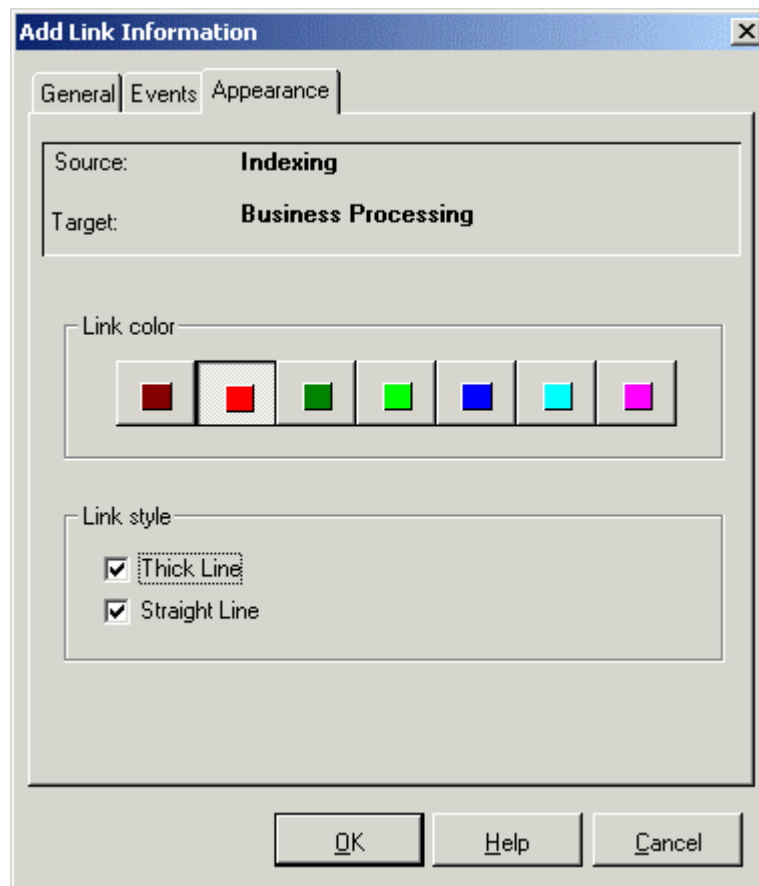


Figure 185: Add Link Information, Appearance tab

For example, a geometrically represented line can become a straight line, or a thick line can become a thin line.

Note: If a DB2 database is used, the selection of link colors is restricted. Colors that are not available are disabled.

7. To assign the link, click **OK**.

A line with a square box in the middle appears between the two nodes with an arrow at one end for a one-way link or both ends for a two-way link. If a link has events assigned to it, this box has a black frame around it.



Figure 186: Created links

8. To modify an existing link, select the **Modify** tool and click on the box in the middle of the link. Make changes as required in the **Modify Link Information** window.

9. To delete a link, select the **Delete** tool and click on the box in the middle of the link.

Exigen Workflow Events

The following events are currently available in Exigen Workflow. A description of each event and its parameters is included. Customized events may be added to accommodate your business practices.

Note: In previous Exigen Workflow versions, Advanced Event Server processed events. Advanced Event Server is replaced by Automatic Queue Server, and Automatic Queue Server handlers can be set up to process events. For more information on Exigen Workflow handlers, see the *Exigen Workflow Administrator's Guide, Part 2: Business Component Reference*, Chapter 21: Exigen Workflow Handlers.

Events are listed alphabetically and described in the following table:

Events	
Assign Documents to Subfolder	
Definition	Locates a subfolder whose field values match the parameters and assigns all documents in the parcel to the subfolder. If no subfolder is found, an error message is displayed. This event works only with default subfolders.
Parameters	Subfolder fields and values, delimited by a comma.
Example	FieldName = FieldValue
Attach page to documents of the defined type	
Definition	Attaches the page specified as a TIFF file to all documents of selected document types. This event works only for DMS files and skips reference documents. Note: This event requires that the DMS COM component is installed.
Parameters	Name and path of a TIFF file to be attached as a cover page, and a list of document types to attach it to.
Example	c:\test\cover.tif, IMAGE, BILL
Audit log housekeeping	
Definition	Cleans up audit records.
Parameters	The following parameters are used: <ul style="list-style-type: none"> • retention time in days • archiving filter ID • export directory • maximum size of exported chunks in kilobytes • flag for record deletion: 1 if deleted, 0 if not deleted • flag for use of export directory: 1 if used, 0 if not used
Example	3, 36, c:\temp, 100, 1, 0
Create Parcel Link	
Definition	Creates a new parcel record and creates references. It does not create copies in that parcel of the documents contained in the original parcel. Multiple parcel links can be assigned.
Parameters	Lists nodes by their internal node ID as shown in the General tab of the node properties and by the user ID where the parcel reference copy is created.
Example	7, DTM, 11, ADM, 14, JON

Events	
Assign Documents to Subfolder	
Match	
Definition	Event goes through the list of nodes that is set in the parameter string, and searches for parcels indexed to the same folder as the event source parcel. If it finds an appropriate parcel, it merges the parcel with the event source parcel and adds the corresponding documents. It deletes the event source parcel.
Parameters	Node identifiers to be checked for matching parcels.
Example	10,11,14
Match and push	
Definition	Event searches the specified node for parcels indexed to the same folder as the event source parcel. If it finds an appropriate parcel, it merges the parcel with the event source parcel, adds the corresponding documents, and pushes the resulting parcel according to the routing rules.
Parameters	Node ID to be searched for matching parcels.
Example	10
Parallel	
Definition	Creates copies of the same parcel, which are assigned to the nodes and users listed in the parameter field. The copies are routed through the workflow, and meet in a rendezvous queue where they are merged.
Parameters	Lists nodes by their internal node ID as shown in the General tab of the node properties and by the user ID to which parallel parcels are sent.
Example	7,DTM,11,ADM,14,JON
Parallel and push	
Definition	Combines the Push and Parallel events to create copies of a parcel and assign them to the target node and user combinations listed in the parameters. It pushes the parcels to the nodes and to the users identified in the routing rules assigned to the target node.
Parameters	Lists nodes by their internal node ID as shown in the General tab of the node properties and the user IDs to which parallel parcels are sent.
Example	7,COM,11,DTM,14,ADM
Pend	
Definition	Merges parcels assigned to the same folder into one when they reach the node to which the event is assigned.
Parameters	Requires no parameters.
Print Parcel Documents	
Definition	Prints the DMS files in each parcel to a designated print server.
Parameters	Printer device name.
Example	PR1
Push	
Definition	Pushes parcels through the workflow based on the routing rules. When a parcel is received in the node to which this event is assigned, the routing rules deliver the parcel to the appropriate node and user. The Push Event eliminates the need to manually send individual parcels.

Events	
Assign Documents to Subfolder	
	Note: If a Push event is assigned to a rendezvous node, received parcels are not pushed immediately. The situation is analyzed every 30 minutes, and when all parcels reach the rendezvous node, it pushes them to the appropriate node and user.
Parameters	Requires no parameters.
Release Folder Work Item	
Definition	Removes reference documents from the existing parcel.
Parameters	Requires no parameters.
Remove Page Notes	
Definition	Removes page notes from each DMS page. This event skips reference documents.
Parameters	Requires no parameters.
Rendezvous	
Definition	Must be used with the Parallel Send command. Parcels that are parallel processed, with multiple instances created and sent to multiple queues and users, must rendezvous at a queue that appears later in the workflow. Once all of the copies are sent to this queue, the rendezvous process occurs and the original parcel is routed to the next workflow queue based on the routing rules. Note that the copies cannot be sent to the next queue until all of them are received and rendezvoused. Note: Use this event when you must collect data and send the data to the next queue without any decision-making. Otherwise, use a queue with rendezvous node type.
Parameters	Requires no parameters.
Route	
Definition	Routes a parcel from one node to another, independent of any links between the source and target nodes. The target node and user are defined in the parameters.
Parameters	Lists the target node by its internal node ID as shown in the General tab of the node properties and the user ID to which a parcel is sent.
Example	7 , DTM
Send e-mail notification	
Definition	Sends a notification via email to the target user selected in the Send Parcel/Document Manager window.
Parameters	Lists the Exigen Workflow user IDs to which the notification is sent. If Outlook® is installed and mail profiles are defined, an Outlook mail profile can be listed as the first parameter. If no Outlook mail profile is listed, the default mail profile is used.
Examples	DTM , ADM , JON PROFILE1 , DTM , ADM , JON
Set cut-off date	
Definition	Sets the current date as the document's cut-off date. A document's cut-off date is the date from which the retention period is calculated for the document.

Events	
Assign Documents to Subfolder	
Parameters	Requires no parameters.
Set Defaults to Folder Fields	
Definition	<p>Updates the values of the folder to which the parcel is sent as specified in the parameters. If no folder exists, one is created and the parcel is assigned to it. Only custom folder fields must be used with this command.</p> <p>The following aliases are used:</p> <ul style="list-style-type: none"> • <code>CUR_DATE</code>: substitute current date and time • <code>NUM_UNQ</code>: substitute unique number for number fields • <code>STR_UNQ</code>: substitute unique string for string fields
Parameters	Folder fields and values, delimited by comma.
Example	<code>FieldName = FieldValue</code>
Set Defaults to Parcel Fields	
Definition	<p>Updates the values of the parcel as specified in the parameters. Only custom parcel fields must be modified with this event.</p> <p>The following aliases are used:</p> <ul style="list-style-type: none"> • <code>CUR_DATE</code>: substitute current date and time • <code>NUM_UNQ</code>: substitute unique number for number fields • <code>STR_UNQ</code>: substitute unique string for string fields
Parameters	Parcel fields and values, delimited by comma.
Split parcel and push	
Definition	Performs the Split Parcel function, which creates a new parcel for each document in the existing parcel and pushes them to the next node or nodes in the workflow based on routing rules. This event is normally used when routing rules are executed at the document level.
Parameters	Requires no parameters.
Submit Folder Work Item	
Definition	Collects all reference documents from the current folder and adds them to the existing parcel.
Parameters	Requires no parameters.

Modifying Workflows in List Mode

The following two alternatives are available for modifying workflows:

Workflow modification modes	
Mode	Description
Graphical mode	<p>Workflow is displayed as a map in the Workflow Map window. The user selects the node or link on the map to modify it.</p> <p>For information on modifying nodes in the Workflow Map window, see Setting Up Workflow Objects.</p> <p>For information on modifying links in the Workflow Map window, see Setting Up Workflow Links.</p>

Workflow modification modes	
Mode	Description
List mode	Workflow is displayed as a list of nodes and links in the Modify Workflow window. The user selects the node or a link on the map to modify it. Tasklists are displayed in list mode by default.

This section describes how to modify workflows in list mode. All types of workflows can be modified in list mode. Nodes can be added, deleted, modified, and sorted in list mode. Links cannot be added or deleted in list mode, but link properties can be modified.

Note: **Modify Workflow** window enhancements are not available in standard Exigen Workflow client/server and Web applications. They are supported by programmable extensions only, and are available via application programming interfaces (APIs). For information on how to acquire this feature, contact Exigen Support Services.

This section describes the following procedures to modify workflows in list mode:

- [Changing Workflow Properties and Access Rights](#)
- [Modifying Nodes and Links](#)
- [Running and Testing a Workflow Object](#)
- [Changing the Node Sort Order](#)

Changing Workflow Properties and Access Rights

To change workflow properties and access rights, proceed as follows:

1. In the **Workflow Builder** window, select the workflow.

2. Click **Modify** .

The **Modify Workflow** window appears.

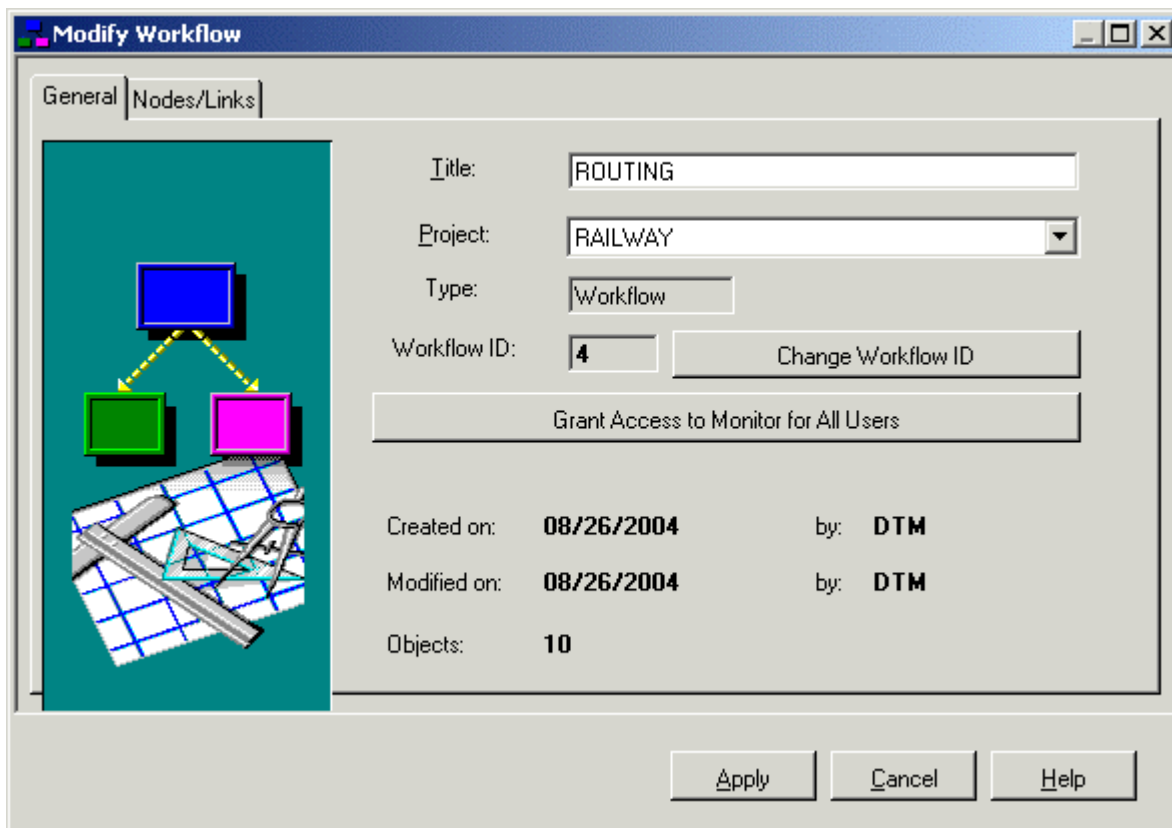


Figure 187: Opening a workflow in list mode

3. To modify the workflow name, select the **General** tab and in the **Title** field, enter a new name.
4. To specify a different workflow project, in the **Project** list, select a new project.

The workflow type cannot be modified.

The **Type** list appears only if Workflow Builder is set up to distinguish between workflow types. For information on workflow types, see [Using Workflow Builder](#).

The workflow ID can be modified, but modification may result in the loss of data. Before modifying the workflow ID, contact the system administrator or Exigen Support Services.

5. To modify the workflow ID, click **Change Workflow ID**.

The **Change Current Workflow ID** window appears.

6. In the **New workflow ID** field, enter an appropriate value.
7. To save the value, click **Apply**.
8. To retain the existing value, click **Cancel**.
9. To grant all users the right to monitor all workflow nodes, click **Grant Access to Monitor for All Users**.

A confirmation window appears.

10. To grant the access rights, click **Yes**.

11. To cancel the action, click **No**.

Modifying Nodes and Links

To modify workflow nodes and links, proceed as follows:

1. Click **Nodes/Links**.

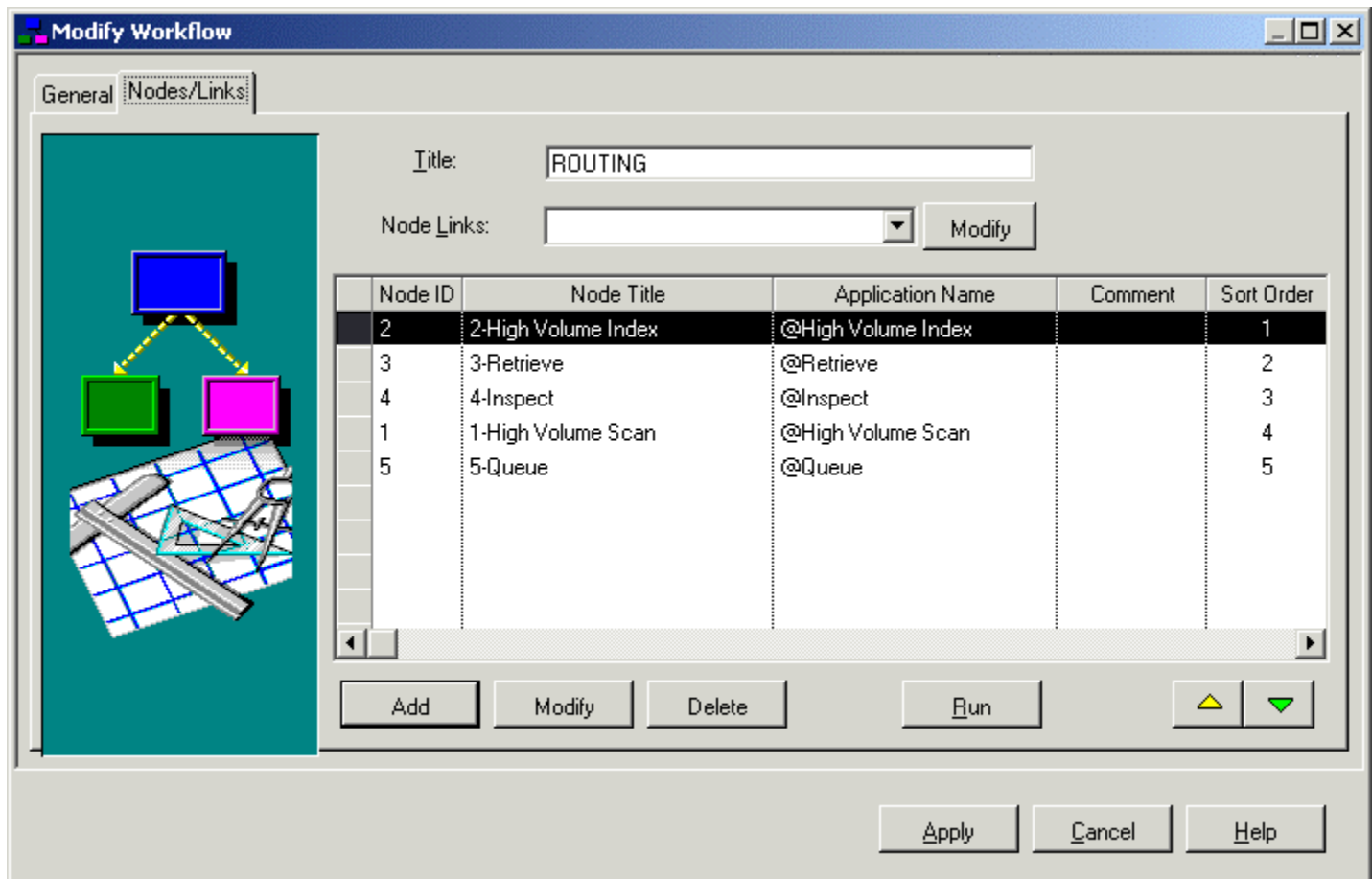


Figure 188: Modifying nodes and links

2. To modify a link, select the link in the **Node Links** list and click **Modify**.

The **Modify Link Information** window appears. The **Modify Link Information** window is similar to the **Add Link Information** window as described in [Setting Up Workflow Links](#).

3. In the **Modify Link Information** window, modify the values as appropriate and click **OK**.

4. To add a node, click **Add**.

The **Add New Node** window appears. Only the object types allowed for the selected workflow type are displayed.

5. Define the node as described in [Setting Up Workflow Objects](#).

The node appears in the table.

6. To modify a node, select it and click **Modify**.
7. In the **Modify Node** window, modify the values.

The **Modify Node** window is similar to the **Add New Node** window. For information on the **Add New Node** window, see [Setting Up Workflow Objects](#).

8. To delete a node, select it and click **Delete**.
9. In the confirmation window, click **Yes**.

Running and Testing a Workflow Object

To run and test a workflow object, proceed as follows:

1. Click **Run**.

The **Select User** window appears.

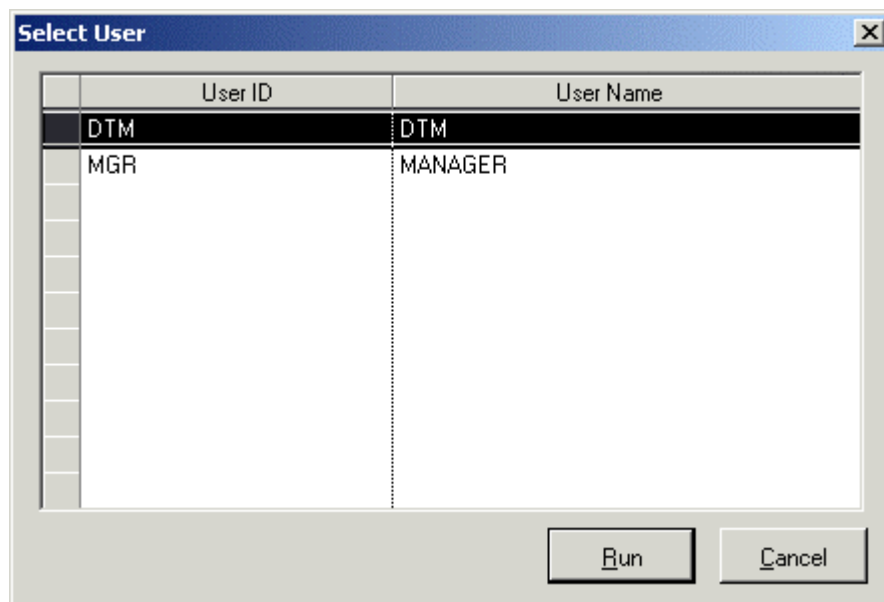


Figure 189: Preparing to run a workflow object

2. In the **Select User** window, select the appropriate user.
3. Click **Run**.

The **Enter Password** window appears.

4. In the **Enter Password** window, enter the user's password.
5. Click **OK**.

The workflow object appears.



6. Test the workflow object as described in [Simulating a Workflow](#).
7. If the test is successful, close the workflow object.

The **Modify Workflow** window appears.

The sort order of nodes in the table can be changed. This is useful when searching for a specific node in a long node list. When the sort order is modified, only the node order in the **Modify Workflow** window changes. The order of nodes in the workflow stays the same.

Changing the Node Sort Order

To change the node sort order, proceed as follows:

1. To move a node up in the list, select the node and click the up arrow .
2. To move a node down in the list, select the node and click the down arrow .
3. To sort the nodes based on a node property, double click the appropriate column name.

For example, to group all nodes associated with a particular application together, **Application Name** is clicked. As a result, all **Inspect** nodes are together and all **Queue** nodes are together.


4. To reverse the sorting order in any sorted column, double click the column.
5. To apply changes and close the window, click **Apply**.
6. To cancel changes and close the window, click **Cancel**.

Using an Alias

An **alias** simplifies the representation of a complicated workflow. An alias of a particular node is a shadow of that node. By drawing links to and from the alias, you are creating links to and from its parent node. This makes your workflow more readable by replacing a web of numerous intersecting links to and from a node with one or several aliases of that node. It also transfers some of the links from the parent node to its aliases.

You can also create links between objects in different submaps by creating one of the object's aliases in another object's submap.

To create an alias, proceed as follows:

1. Click the **Alias** tool .
2. Position the pointer where you want to add the alias and click.

The **Select Alias** window appears, listing all nodes in the workflow.

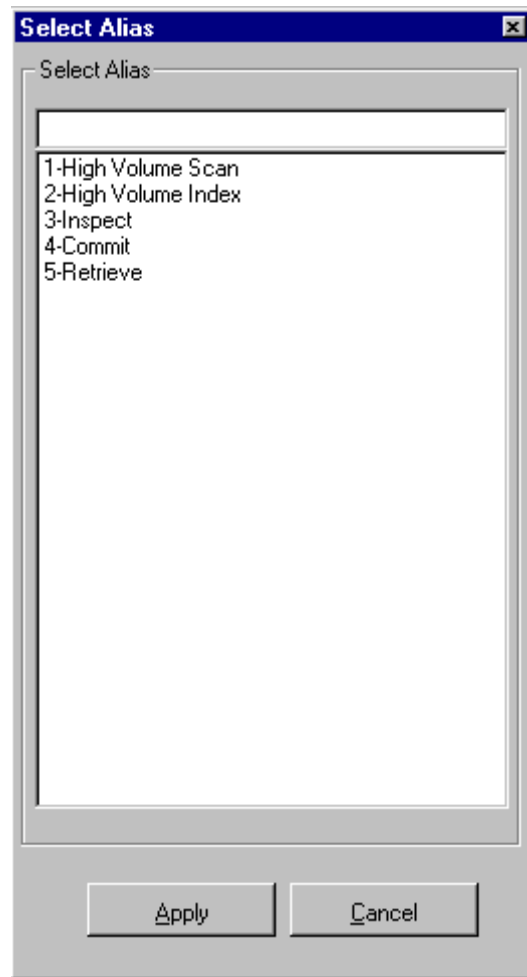


Figure 190: Creating an alias

3. Select the node you want to represent with an alias and click **Apply**.

The alias appears as if it were the actual node, except that the title defines it as an alias. The alias node icon has a green marker in the lower-right corner.



Figure 191: Created alias

Nodes with an alias are identified by a red marker in the top-left corner of the node icon.



Figure 192: Node with an alias

4. To continue plotting your workflow map, add links from nodes to the alias as required.

Using a Case

The **Case tool** allows you to improve the clarity of your workflow map. For example, if you have several nodes with several outgoing links, representation is difficult to understand. This tool is also useful if, in a given node, two users process the same document at different times; for example, one user works with it in the morning, and the other works with it at night. You need to send the document from and to the same node.

To use the Case tool, proceed as follows:



1. In the **Workflow Builder** toolbar, click the **Assign Case** tool.
2. Position the pointer next to the node that has several outgoing links and click.
3. Connect the node with the **Case**.
4. Create links from the **Case** to all nodes connected with that node.

Note: Double-linking to **Case** is not supported.

Creating a Submap

A submap must be created when the workflow map is too complicated or too large. As the number of nodes and links increases, the ability to read the map decreases. Submaps can be used to represent a group of nodes on another map while retaining links to the main map.

To create a submap, proceed as follows:



1. Click the **Submap** tool.
2. Position the pointer over the workflow and click.
3. Enter the submap name and click **OK**.

The submap is represented on the main workflow map.

4. To open the submap, click the **Grabber** or **Modify** tool and click on the submap icon.

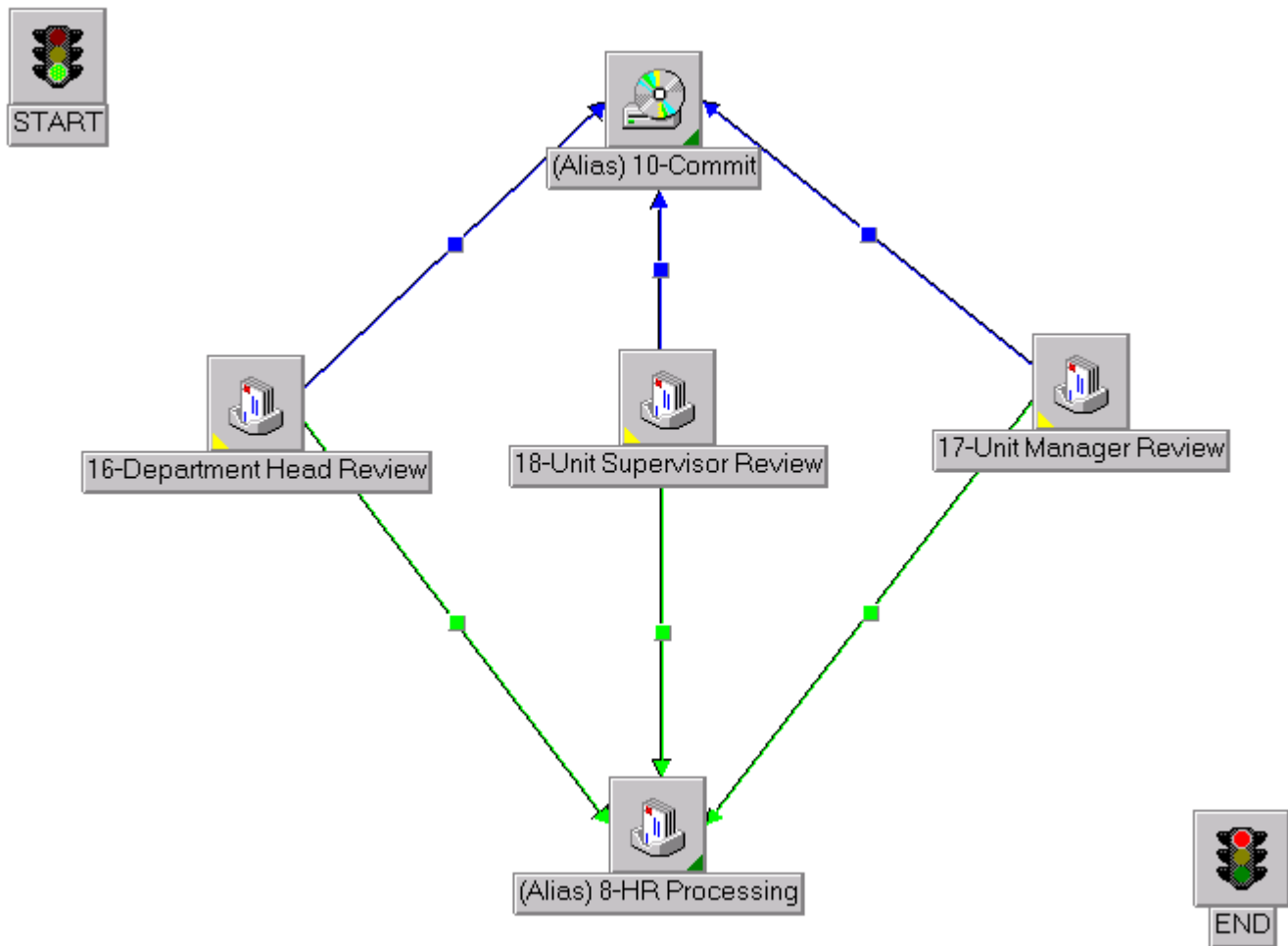


Figure 193: Creating a submap

A new workflow map window appears with the submap name as the title. A green light appears at the top left and a red light at the lower right.

5. Use these lights to link nodes from the previous map to nodes in the submap.
You can also use aliases to perform this function. For information on aliases, see [Using an Alias](#).
6. Add nodes, links, aliases, and other submaps to represent your business processes in the submap.
7. When finished, to the main workflow map, select the **Stop Light** to return.
8. To change the name of a submap, click the **Modify** tool and click on the submap icon.
9. To delete the submap, click the **Delete** tool.

Setting Up Workflow Routing Rules

After you place nodes, links, and submaps on the main workflow map, you can add routing rules to facilitate the document routing process. The **Rules** tab in the **Add New Node** window is disabled when adding a new node, but is enabled once a node is in place. It is not possible to add or modify routing

rules if the workflow is currently in use. If an attempt is made to add or modify routing rules for a workflow in use, an error message is displayed.

Routing rules consist of IF statements. Statements that use table fields, table values, and destination queues and users are conditional.

A final ELSE statement routes any parcels that do not satisfy the IF conditions.

To add routing rules, proceed as follows:

1. Click the **Rules** tool  or, in the **Modify Node** window, select the **Rules** tab.

If you click the **Rules** tool, the **Workflow Routing Rules** window appears.

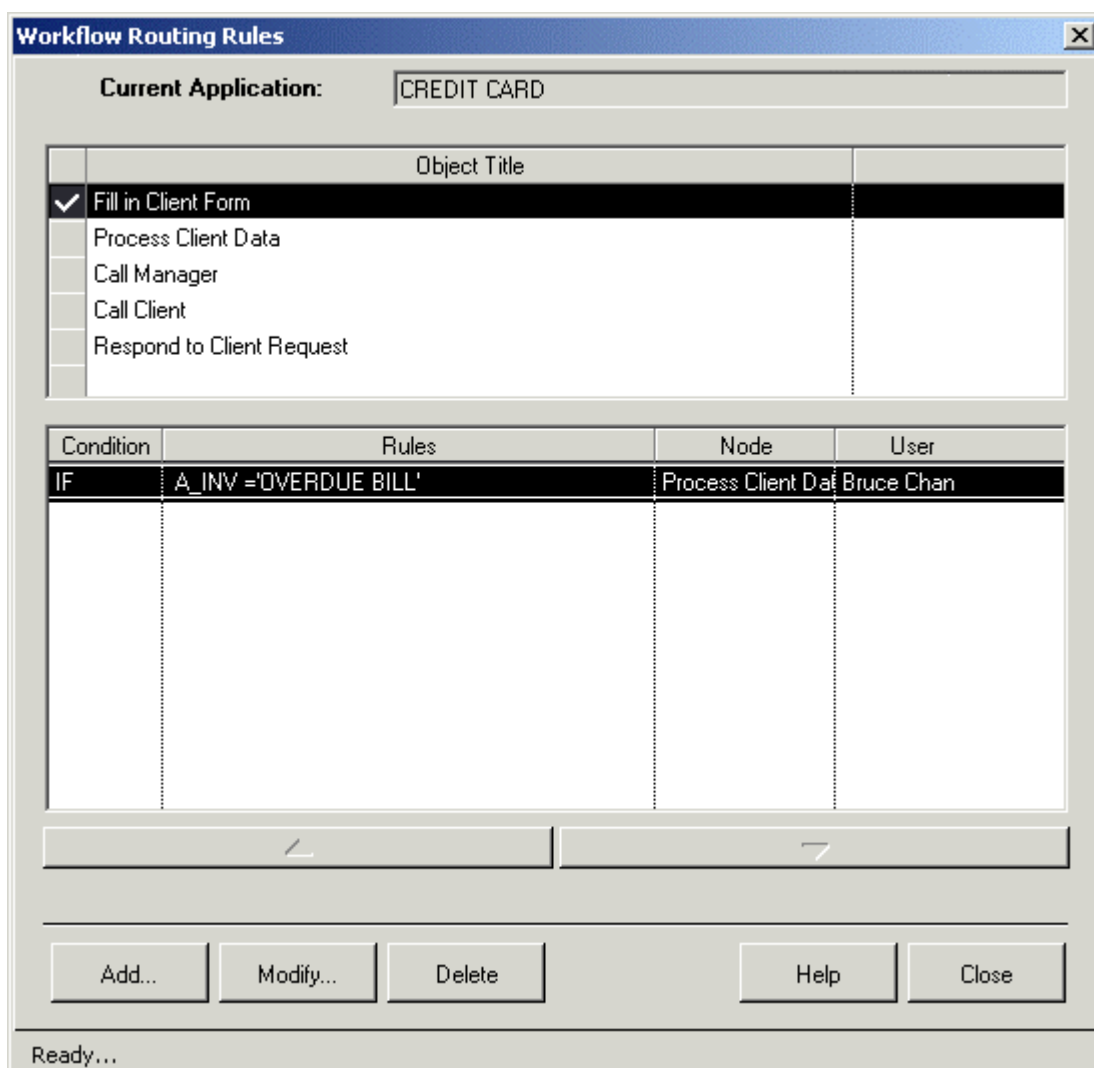


Figure 194: Workflow Routing Rules window

If you select the **Rules** tab, the **Modify Node** window displays the **Rules** tab.

Modify Node

Monitor | E-Forms | Taskflow | Additional Settings

General | Form | **Rules** | Send | Escalation

Workflow object: @High Volume Scan 1

Desktop title: 1-High Volume Scan

Condition	Routing Rules	Route to Node	Route to User
-----------	---------------	---------------	---------------

Add new Rule...

Group Maint. Apply Help Close

Figure 195: Modifying a node, Rules tab

The table displays the rules in the current node.

2. To add a rule, in the **Workflow Routing Rules** window, click **Add**, or, in the **Rules** tab, click **Add new Rule**.

The **Add Routing Rule** window appears.

Add Routing Rule

(1) Table/Field Selection

Select a level: **DOCUMENT**

Select a field:

Field	Type
DOC_RSN	INTEGER
DOC_SCAN_DATE	DATETIME
DOC_TYPE	VARCHAR
DOC_DESC	VARCHAR
FLD_RSN	INTEGER

(2) Conditional Statement

☒ IF ☐ ELSE

DOC_TYPE = 'BILL'

(3) Route to

Queue: **Process Client Data**

User: **DTM**

(4) Conditionals

= <= >= <>
 < > ()
 AND OR

Verify Help Close

Click to select the send-to user...

Figure 196: Adding a rule

- In the **Select a level** list, select the table that contains the field that your new rule is based on. The following tables are listed:
 - FOLDER
 - SUBFOLDER
 - BATCHPARCEL
 - DOCUMENT
 - COMBINATION

COMBINATION is used to select a combination of tables.

When the table is selected, its fields are displayed in the **Select a field** section.

- To place a field into the **Conditional Statement** area, double click on the field.

The default radio button is IF. If you are adding an ELSE statement, you do not need to select a level or field, or specify conditions.

- To add the condition after the field name, click the **Conditionals** buttons or press the appropriate key.

6. Enter the values for the routing criteria.

Routing rules can be simple or complicated, depending on your individual needs.

OR statements must be enclosed by parentheses to enable correct routing.

The following examples demonstrate incorrect and correct rule syntax:

Incorrect rule:

```
DOC_TYPE = '1' OR DOC_TYPE = '2'
```

Correct rule:

```
(DOC_TYPE = '1' OR DOC_TYPE = '2')
```

7. When the condition is created, select the queue and user to whom the parcels are to be sent.
8. To add the rule, click **Verify**.
9. After the rules are added, to change the order of the IF statements, in the **Rules** tab, click **Up** and **Down**.

Note: **Up** and **Down** buttons appear in the window after closing and reopening it.

Once a statement is satisfied, the parcel is routed to its corresponding queue and user. The ELSE statement must be listed last.

After rules are added to a node, the node icon is identified by a blue marker in its upper-right corner.

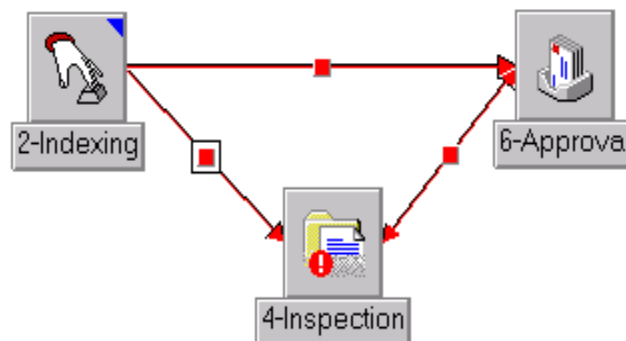


Figure 197: Node with rules

10. To modify a rule, select the rule and click **Modify**.
11. To remove a rule, select the rule and click **Delete**.
12. To close the window, click **Close**.

Note: It is possible to use hidden stored procedures in Exigen Workflow routing rules scripts. However, it is strongly recommended that you avoid these procedure calls, because they are not supported by several Exigen Workflow components, such as Application Services. In addition, import and export procedures do not support stored procedures. Using the stored procedures can also lead to incompatibility with future Exigen Workflow releases.

Integrating with Exigen E-Forms

Exigen Workflow enables integration with Exigen E-Forms. The integration allows viewing, creating, and editing electronic forms from within Exigen Workflow.

Note: You must have administrator rights to perform this operation.

To integrate Exigen E-Forms with Exigen Workflow, proceed as follows:

1. To create E-Forms tables, select **Exigen Workflow Explorer > Administration Tools > Database Tools > Project Builder**.
2. From the menu, select **Project > Create E-Forms Tables** for the project in which you want to use Exigen E-Forms.
3. Ensure that the path to the Exigen E-Forms server is specified as described in [E-Forms Tab](#) in [Configuring the Project](#).
4. Create a queue node in the Workflow Builder for a workflow in which you want to use Exigen E-Forms.
5. In the **E-Forms** tab, enter appropriate values.

[illegible]

Figure 198: Modify Node window, E-Forms tab

6. In the **Modify Node** window, specify any actions to be performed with forms.
7. To add a new action, click **Add new Action**.

The **Action** window appears.

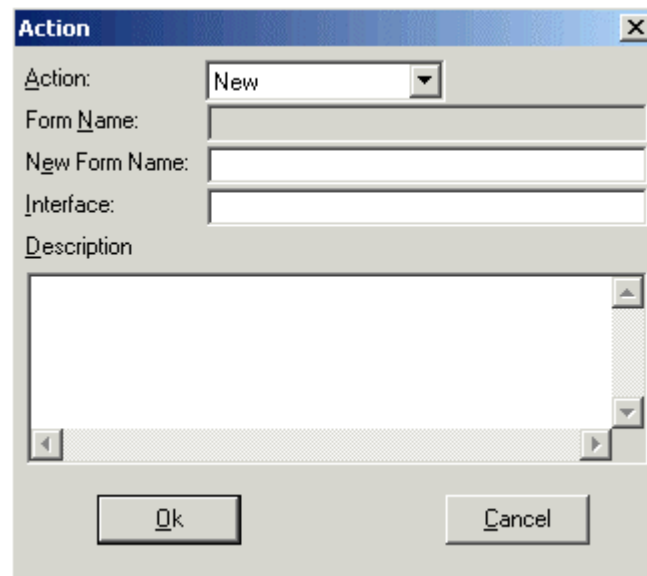


Figure 199: Action window

8. In the **Action** list box, select an action.

The following actions are available:

E-Forms actions	
Action	Description
Attach	Attaches a new form to an existing parcel.
Copy	Creates a form filled with data copied from another form.
New	Launches a form.

9. In the corresponding fields, enter the form name, new form name, and the opened interface.

Depending on the selected action, either the **Form Name** field or the **New Form Name** field is disabled.

10. In the **Description** field, enter the form's description.

Do not leave this field empty, because this description is used later in the user interface to identify forms.

11. Click **OK**.

The new action is available in the corresponding workflow node. As a result, the workflow node window has one or more new buttons for managing forms depending on which actions are added.

12. To modify existing actions, click **Modify Action** and enter appropriate values.

13. To delete an action, click **Delete Action**.

Using an Oracle Stored Procedure for the Common Queue

Exigen Workflow enables a special Oracle database specific stored procedure to be used, which must be written by an administrator. This procedure is called by the **Get From Com** function, and it enables a user to define what the next work item is from the common queue.

The stored procedure is available only if you are using an Oracle database for Exigen Workflow.

The administrator must write the procedure and set it up in the **Form** tab of the **Modify Node** window. The following sections describe how to write and use the procedure:

- [Creating a Stored Procedure](#)
- [Setting Up a Stored Procedure](#)

Creating a Stored Procedure

To create a stored procedure for an Oracle database, use the following declarations for parameters:

Oracle database stored procedure	
Parameter	Description
WfIID IN NUMBER	Workflow ID.
NodeID IN NUMBER	Node ID.
UserID IN NUMBER	Exigen Workflow user ID that is assigned the next work item.
CommUser IN VARCHAR2	Common user ID.
NextWorkItem OUT NUMBER	ID of next work item or an error code.
ErrorMessage OUT VARCHAR2	Error message text that is displayed to the user if the NextWorkItem contains an error code.

The following rules apply when creating this stored procedure:

- If there are no work items, the stored procedure must set `NextWorkItem` to `NULL`.
- If `NextWorkItem` is set to a negative value less than -1, it is assumed to be an error code. A message box with the stored procedure name, error code, and error message is displayed.
- If there are SQL errors in the stored procedure or the stored procedure call fails, a standard SQL error dialog is displayed.

Setting Up a Stored Procedure

Exigen Workflow must be configured to use the stored procedure written by an administrator.

To enable Exigen Workflow to use the stored procedure, proceed as follows:

1. Start Workflow Builder.
2. Double click a workflow.
3. Double click a node in the workflow map.

The **Modify Node** window appears.

4. Select the **Form** tab.

The screenshot shows the 'Modify Node' window with the 'Form' tab selected. The window has a title bar 'Modify Node' and a close button. Below the title bar are tabs: 'Monitor', 'E-Form', 'Taskflow', and 'Additional Settings'. Under 'E-Form', there are sub-tabs: 'General', 'Form' (selected), 'Rules', 'Send', and 'Escalation'. The 'Form' tab contains the following fields and controls:

- 'Workflow object:' text box with '@Inspect' and a spinner box with '1'.
- 'Desktop title:' text box with '1-Inspect'.
- 'Form executable:' text box with a browse button ('..').
- 'Form parameter:' text box with a browse button ('..').
- 'Auto load' checkbox, which is unchecked.
- 'Clear All' button.
- 'Enable stored procedure' checkbox, which is unchecked.
- 'Stored procedure for a common queue:' text box.

At the bottom of the window are three buttons: 'Apply', 'Help', and 'Close'.

Figure 200: Modify Node window

5. Select the **Enable stored procedure** check box.
6. In the **Stored procedure for common queue** field, enter the name of the stored procedure.

The indication about using a stored procedure in an Exigen Workflow object appears in the **Define Queue Settings** window that is opened by selecting **Work > Define Queue Settings**.

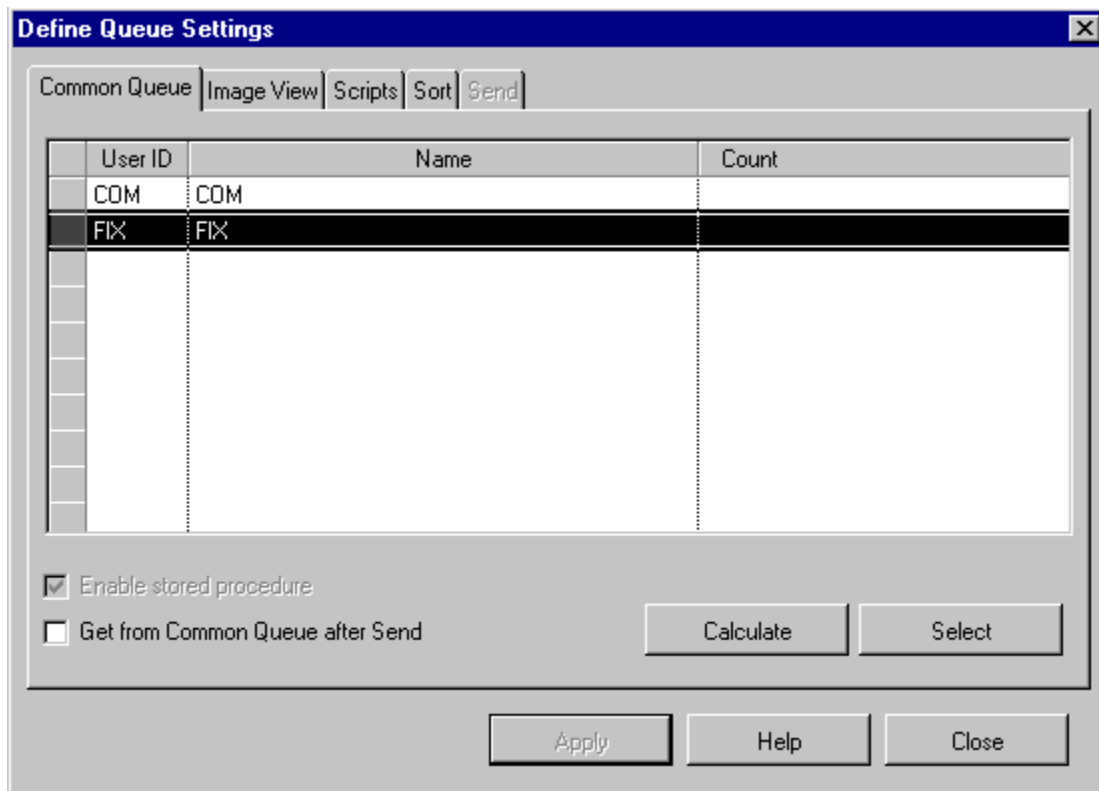


Figure 201: Define Queue Settings window

Simulating a Workflow

The Workflow Simulator function tests the workflow and logs into multiple queues as multiple users. You do not have to exit the workflow currently being created or modified to use this feature. The Simulator uses live data and processes jobs as if multiple users are working.

To test the workflow, proceed as follows:

1. Click **Simulator Mode**.

The workflow is saved and all buttons in the **Workflow Map** window are disabled.

2. Double click on the node to test.

The **Select User** window appears. Only the users with access to this node are listed.

3. Select the user login to simulate and click **Run**.

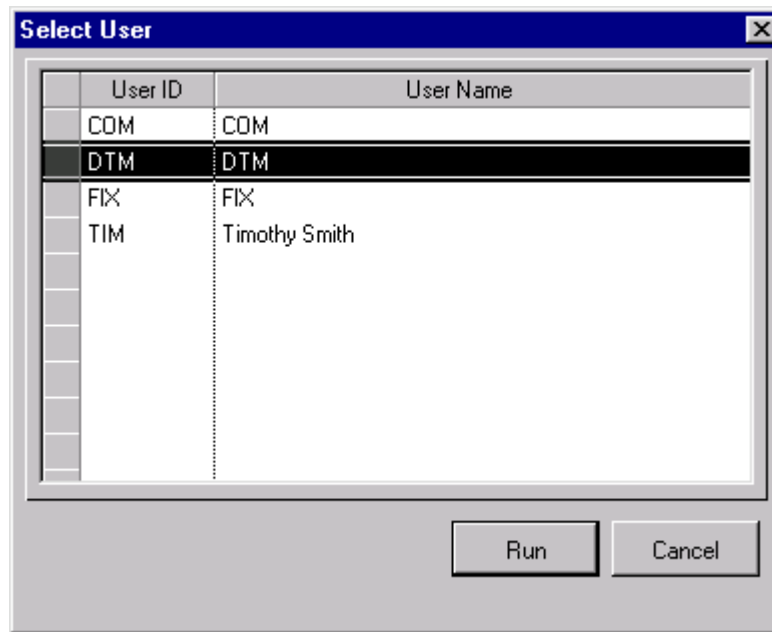


Figure 202: Simulating a workflow, selecting a user

If you have chosen a user name that differs from your current login, the **Enter Password** dialog appears.

4. Enter the password for this user and click **OK**.

The password is saved for the current session.

The selected node appears as normal and you can test the workflow links and routing rules assigned to the current node. When you finish testing and close the node, the workflow map reappears in Simulator mode, allowing you to proceed with any additional workflow testing.

5. To return to the **Workflow Builder** mode, click **Simulator Mode** again.

Using Designer Mode

Designer mode is used to create and modify task checklists and interaction scripts tasks used with Task Oriented Workflow.

For information on using the Workflow Builder **Designer Mode** button, see the *Task Oriented Workflow Administrator's Guide*, Chapter 3: Creating a Taskflow, Creating and Modifying Interaction Script Tasks and Task Checklists.

Using the Hidden Mode Feature

While submaps are useful in simplifying your workflow map, it can still be difficult to identify some target nodes. The **Hidden Mode** feature allows you to view outgoing links for a selected node.

To use the Hidden Mode feature, proceed as follows:

1. Select **Mode > Hidden Mode**.

All links change to gray.

2. Click on a node.

The outgoing links are displayed in their respective color.

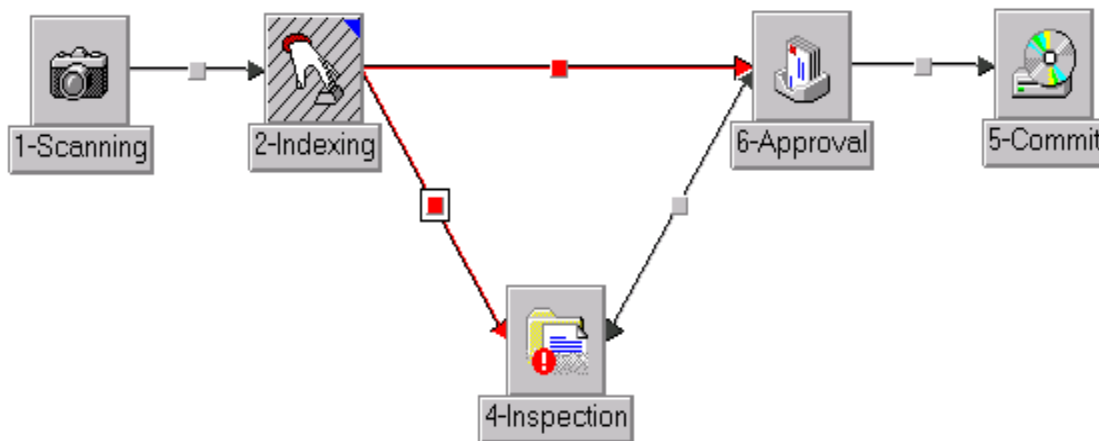


Figure 203: Hidden mode

Setting Viewer Focus

In the High Volume Index, Queue, Inspect, and Low Volume Scan nodes, the primary focus can be set on the node window or the Image Viewer. The focus determines which window is initially activated and displays system messages.

To set the focus, proceed as follows:

1. In the Windows system directory, open the `visiclt.ini` file.

For each node type, viewer focus is set by adding a parameter to the appropriate section of the `visiclt.ini` file as follows:

visiclt.ini file sections for setting viewer focus	
Node type	File section
High Volume Index	[setup_index]
Queue	[setup_queue]
Inspect	[setup_inspect]
Low Volume Scan	[setup_setupscan1]

2. To set viewer focus for a node type, in the appropriate section, add the following line:

```
viewer_focus=
```

3. To place the focus on the node window, enter 0 .
4. To place the focus on the Image Viewer, enter 1 .
5. Save and close the `visiclt.ini` file.

Tips for Building a Workflow

- To see all links to and from any node, right click on the node. This also includes Ad hoc group links, which are not visually shown on the map.
- To perform background processes in the workflow, set up Automatic Queue Server to perform background processes as described in the *Exigen Workflow Administrator's Guide, Part 2: Business Component Reference*, Chapter 19: Automatic Queue Server.
- To pass documents forward without performing checks on them, define only an ELSE condition in the routing rules.
- When defining routing rules for a background process, include an ELSE condition. If there is an ELSE condition and if there is a document that does not correspond to your conditions, it is routed to another queue and is not held in the background queue.
- If appropriate, use two common users in one group. For example, if a team of indexers has two underlying teams, one indexing last names starting with A-M and the other indexing names starting with M-Z, each team knows that they must pull documents from the corresponding common user.
- Do not use common users if users are using the Auto Send feature. When a user sends the processed document to the next node, he or she selects Auto Send from the list of users. This feature distributes work evenly among the users of the next node. The document is routed to the user with the smallest number of pending work items.
- To ensure that the **Workflow Builder** window is the same size and appears at the same position next time it is opened, click **Save Configuration**.



Exporting and Importing a Workflow

A workflow can be exported from a project and imported into another project.

Exporting a Workflow

To export a workflow, proceed as follows:

1. In Exigen Workflow Explorer, select **Administration Tools > Workflow Tools**.
2. Double click Workflow Builder.

The **Workflow Builder** window appears.

3. In the **Workflow Builder** window, select a workflow for export.
4. Select **File > Export Workflow**.

The **Export Workflow** dialog appears.

The **Export file and location** field displays the default location and file name for the exported file.

5. To select another location and file name, click the browse button next to the **Export file and location** field.

The **Export Workflow – Open File** dialog appears.

6. After selecting a new folder and file name, click **Save**.

The **New workflow name** field displays the name of the workflow selected for export.

7. To select a different name for the workflow to be exported, enter a new name in the **New workflow name** field.
8. In the **Note** field, enter an optional note on the workflow.
9. Click **Start Export**.
10. To view or edit the exported file, click **Read File**.
11. To close the **Export Workflow** window, click **Close**.

The file is available at the selected location with the file name extension `.wfl`.

The following table describes the **Export Workflow** window:

Export Workflow window	
Name	Description
Current project name	Currently selected project name.
Current workflow name	Currently selected workflow.
Export file and location	Exported file name and location. This field is editable.
New workflow name	Exported workflow name. By default, the name matches that of the current workflow. This field is editable.
Note	Optional note.
Start Export	Initiates the export process.
Read File	Opens the exported script file in the Notepad text editor for viewing and editing.
Help	Opens help.
Close	Closes the window.

Importing a Workflow

An exported workflow can be imported into another project. The imported workflow can be added to the project or can replace a workflow in the project.

For information on exporting a workflow, see [Exporting a Workflow](#).

To import a workflow, proceed as follows:

1. In Exigen Workflow Explorer, select **Administration Tools > Workflow Tools**.
2. Double click Workflow Builder.

The **Workflow Builder** window appears.

3. Select **File > Import Workflow**.

The **Import Workflow** dialog appears.

4. In the **Import file and location** field, enter the file name and location from which the workflow is imported. To select the file name and location, click the browse button next to the **Import file and location** field.

The **Import Utility – Open File** dialog appears.

5. In the **Import Utility – Open File** dialog, select the file to be imported.

The file must have `.wfl` as its file name extension.

6. Click **Open**.

The **Workflow name** field initially displays the name of the source workflow. This name can remain unchanged.

7. To change the name of the workflow, in the **Workflow name** field, enter a different name.
8. To replace an existing workflow with an imported workflow, click the arrow next to the **Workflow name** field and select the workflow to be replaced.
9. To select the name of the project into which the workflow is imported, click the arrow next to the **Project name** field and select a name.
10. Click **Start Import**.

If you selected an existing workflow, you are asked whether to replace it.

11. To replace the workflow, click **Yes**. To cancel replacement, click **No**.

After the import is completed, the **Users in Groups** dialog appears.

The **Users in Groups** dialog indicates whether additional users must be added to any user group for the imported workflow. For more information on the **Users in Groups** dialog, see [Users in Groups Dialog](#).

12. To close the **Users in Groups** window, click **Close**.

The following table describes the **Import Workflow** window:

Import Workflow window	
Name	Description
Import file and location	Import script file name and location.
Source name	Workflow from which the script was created.
Workflow name	New workflow name. The current workflow name is the default name.
Project name	Project in which the workflow is to be imported.
Notes	Notes on the workflow to be imported.
Start Import	Initiates import.
Read File	Opens the imported script file in the Notepad text editor for viewing and editing.
Help	Opens help.
Close	Closes the window.

Users in Groups Dialog

The **Users in Groups** dialog appears after a workflow is imported. The dialog displays the user groups that were created as a result of workflow import and indicates whether any users must be assigned to user groups.

The following table describes the **Users in Groups** dialog:

Users in Groups dialog	
Name	Description
Users to be registered	Users that must be registered in Administration Tools to ensure that the workflow functions properly.
Workflow groups	Workflow groups created during the workflow import process.
Users in group	Users in a user group. User names appearing in red must be assigned to user groups.
Close	Closes the dialog.

Managing Components

Component Configuration Manager is a tool that creates and manages workflow components.

The following table describes the component types managed with Component Configuration Manager:

Component Configuration Manager component types		
Type	Description	Example
plugin	Code reference and configuration data for processing an event. A plugin can contain a code reference or configuration data, or both.	A plugin contains a reference to code that is executed to retrieve a work item, and a document type to be displayed. For example, only invoices are retrieved and displayed.

Component Configuration Manager component types		
Type	Description	Example
application	Reusable activity in a workflow.	Application is used to index incoming documents or to process a customer complaint using an interaction script.
reusable node	Business activity or set of activities performed by a person or an automatic process as part of the workflow.	A node is used to generate invoices for an automobile manufacturer.

Note: Component Configuration Manager is not available in standard Exigen Workflow client/server and Web applications. It is supported by programmable extensions only, and is available via application programming interfaces (APIs). For information on how to acquire this feature, contact Exigen Support Services.

Component Configuration Manager uses inheritance to create child components from parent components. Settings that are specified once in a parent component can be reused as often as required. For example, if the parent component is an application that generates invoices for customers in Australia, a child application generates invoices for customers in the United States. The two applications are similar, but the generated invoices have different address formats to accommodate regional differences.

Only one instance of Component Configuration Manager can be active at a time.

The following topics are included in this section:

- [Starting Component Configuration Manager](#)
- [Component Configuration Manager Window](#)
- [Adding a New Component](#)
- [Adding a New Component from a Component](#)
- [Adding an Existing Component from a Component](#)
- [Adding an Inherited Component](#)
- [Removing a Component](#)
- [Exporting Component Configurations](#)
- [Importing Component Configurations](#)
- [Viewing and Modifying a Component](#)
- [Component Configuration Manager Window Buttons and Menu Commands](#)

Starting Component Configuration Manager

If Component Configuration Manager must be launched from a network share, ensure that one of the following conditions is met:

- All three Component Configuration Manager assemblies are assigned the full trust level.
- All local intranet security zone assemblies are assigned the full trust level.

To start Component Configuration Manager, proceed as follows:

1. To configure settings for a project, perform one of the following steps:
 - In Exigen Workflow Explorer, select **Administration Tools > Workflow Tools** and double click

Component Configuration Manager .

- In the C:\VisiFLOW\SYSTEM directory, run MENUCCM.exe, enter the user name and password, and click **Connect**.
- Open Workflow Builder, double click a workflow, and click **Component Configuration Manager**



2. To configure settings for a workflow node, proceed as follows:
 1. Open Workflow Builder.
 2. To open a workflow, double click it.
 3. Double click the node.

4. Click .

If a project is not selected, the **Select Project** window appears.

3. If the **Select Project** window appears, in the **Project** list, select a project.

Configuration settings apply only to the selected project.

4. Click **Ok**.

Each configuration requires a schema, which defines the configuration structure, and a component dictionary. If the schema and component dictionary are not specified, the **Import New Schema** window appears.

5. To select a schema, in the **Import New Schema** window, next to the **Schema File Name** field, click **Browse**.
6. In the **Open** window, select the following schema:

`\VisiFLOW\SYSTEM\CfgSchemas\WorkflowBase.xsd`

7. Click **Open**.
8. To select a component dictionary, in the **Import New Schema** window, next to the **Component Dictionary File Name** field, click **Browse**.
9. Select the following component dictionary:

`\VisiFLOW\SYSTEM\CfgSchemas\ComponentDictionary.xml`

10. Click **Open**.
11. Click **Ok**.

The **Component Configuration Manager** window appears.

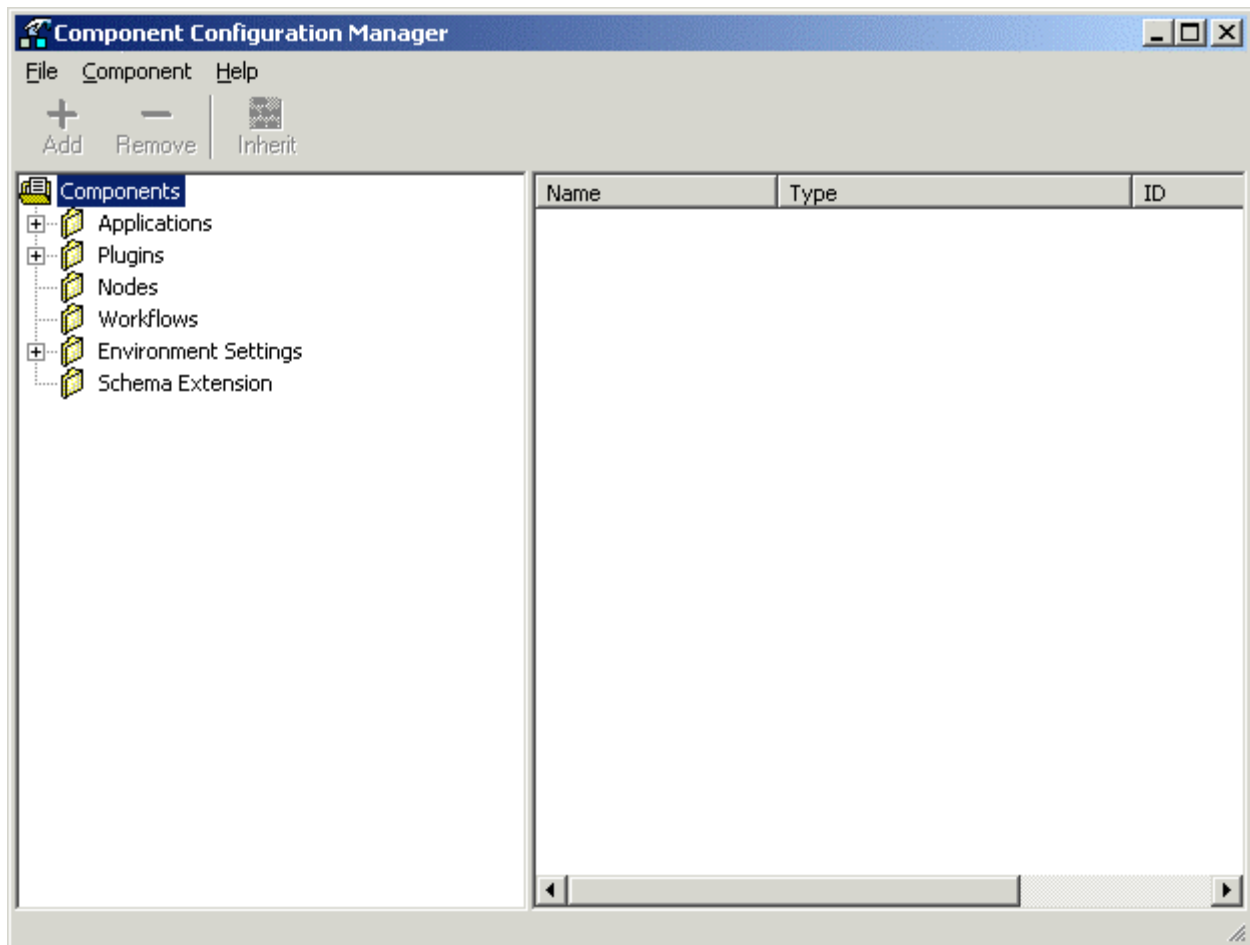


Figure 204: Opening Component Configuration Manager

Component Configuration Manager Window

The **Component Configuration Manager** window displays component types in the left pane and component details in the right pane.

A full list of component types and subtypes is displayed by clicking + next to the elements in the component types tree.

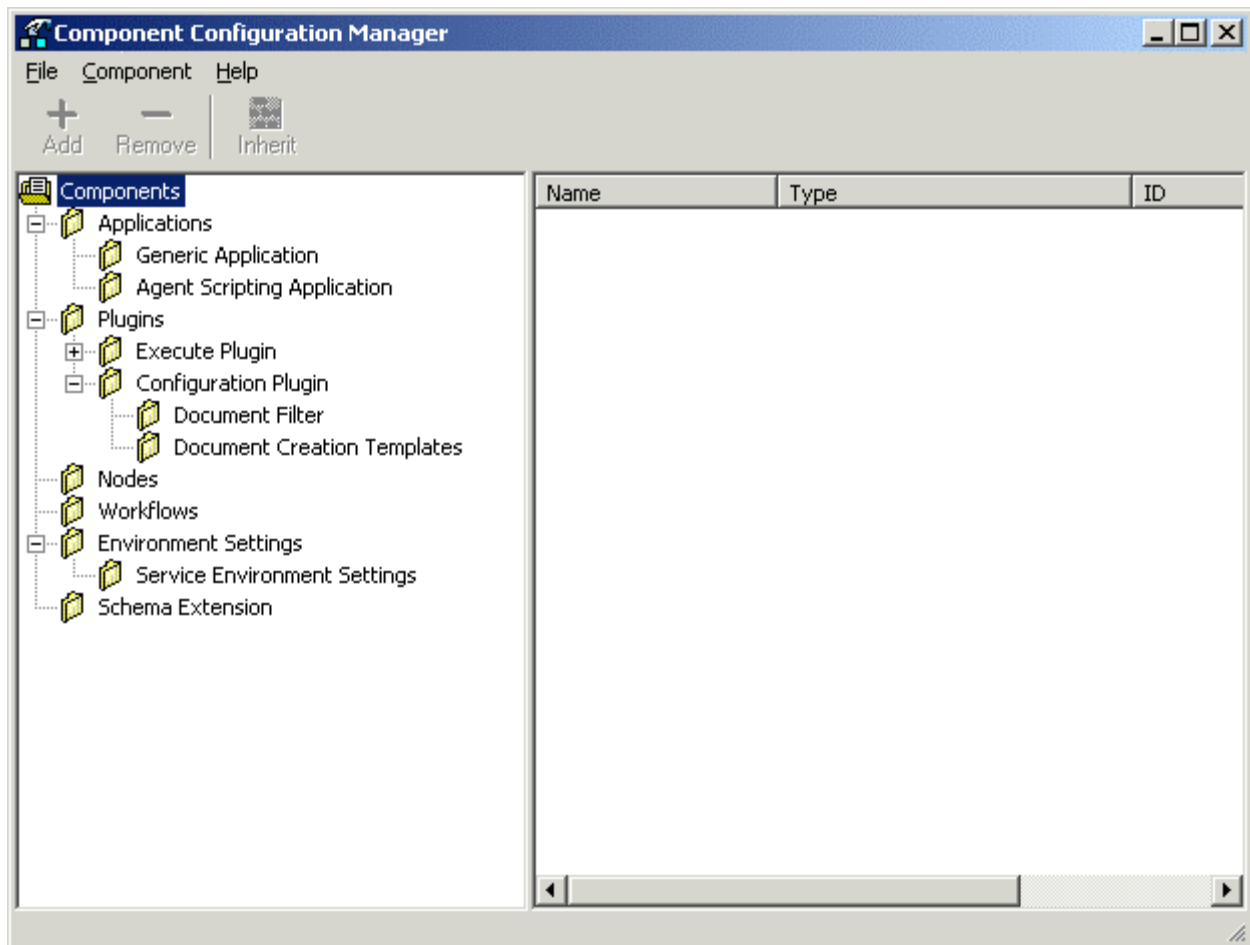


Figure 205: Viewing component types

The following topics are included in this section:

- [Component Types and Subtypes](#)
- [Component Attributes](#)

Component Types and Subtypes

The following table describes component types and subtypes displayed in the tree:

Component types and subtypes		
Type	Subtype	Description
Applications	Generic Application	Reusable activity such as scanning or indexing documents.
Applications	Agent Scripting Application	Reusable activity supported by Exigen Interaction Scripting.

Component types and subtypes			
Type	Subtype	Description	
Plugins	Execute Plugin	Generic executable plugins.	
		The following execute plugin subtypes are available:	
		Subtype	Description
		Entry Routing Rule	Specifies actions performed on a workitem that enters a node.
		Exit Routing Rule	Specifies actions performed on a workitem that exits a node.
		Workitem Initialization	Specifies custom code for workitem initialization.
		Create Workitem	Specifies default values for creating a task workitem.
		Workitem Prioritization	Specifies rules for pulling a workitem from a common queue.
		Workitem Parallel Send	Specifies workitem processing when parallel workitem instances are created but are not yet sent.
		Workitem Rendezvous	Specifies merge logic when parallel workitem instances are merged in a rendezvous node.
Plugins	Configuration Plugin	Configuration plugins.	
		The following configuration plugin subtypes are available:	
		Subtype	Description
		Document Filter	Specifies the document types available to the application. For example, a document filter is defined to ensure that only invoices enter a document node for processing invoices.
		Document Creation Templates	Specifies the document type and template for document creation. For example, if a node is used for invoice generation, an invoice template is specified. The invoice template is opened automatically when the user creates a new document.
Nodes		Reusable business activity or set of activities. No subtypes are defined.	

Component types and subtypes		
Type	Subtype	Description
Workflows		List of workflows. The list is read-only.
Environment Settings	Service Environment Settings	Web Services configuration.
Schema Extension		Component Configuration Manager custom user interface configuration.

Component Attributes

Each component is assigned attributes. The following table describes component attributes:

Component attributes		
Attribute	Description	Example
Name	Name that describes the component's purpose.	U.S. Invoice Creation
Type	Component type.	Node
ID	Unique component identifier. It is assigned automatically when the component is created.	988b8017-3f43-433e-880c-4fe7a93a9349
Inherited From	Reference to the parent component.	Invoice Creation

For a description of the **Component Configuration Manager** window buttons and menu commands, see [Component Configuration Manager Window Buttons and Menu Commands](#).

Adding a New Component

To add a new component using Component Configuration Manager, proceed as follows:

1. To add a component definition, in the left pane, select the component type or subtype.

The **Add** button is enabled only when an available component type or subtype is selected.

2. Click **Add** .

The **Add New Component** window appears. The selected component type or subtype is displayed in the **Component Type** field.

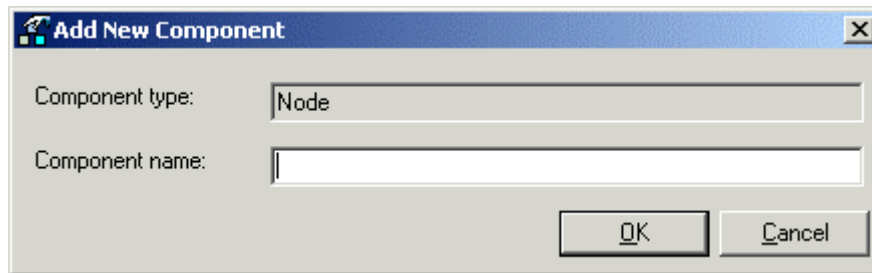


Figure 206: Adding a component

3. In the **Component Name** field, enter a component name.
4. Click **OK**.

The **Component Viewer** window appears. It is used for viewing and specifying component properties. The displayed property pages and tabs differ, depending on the component type and subtype.

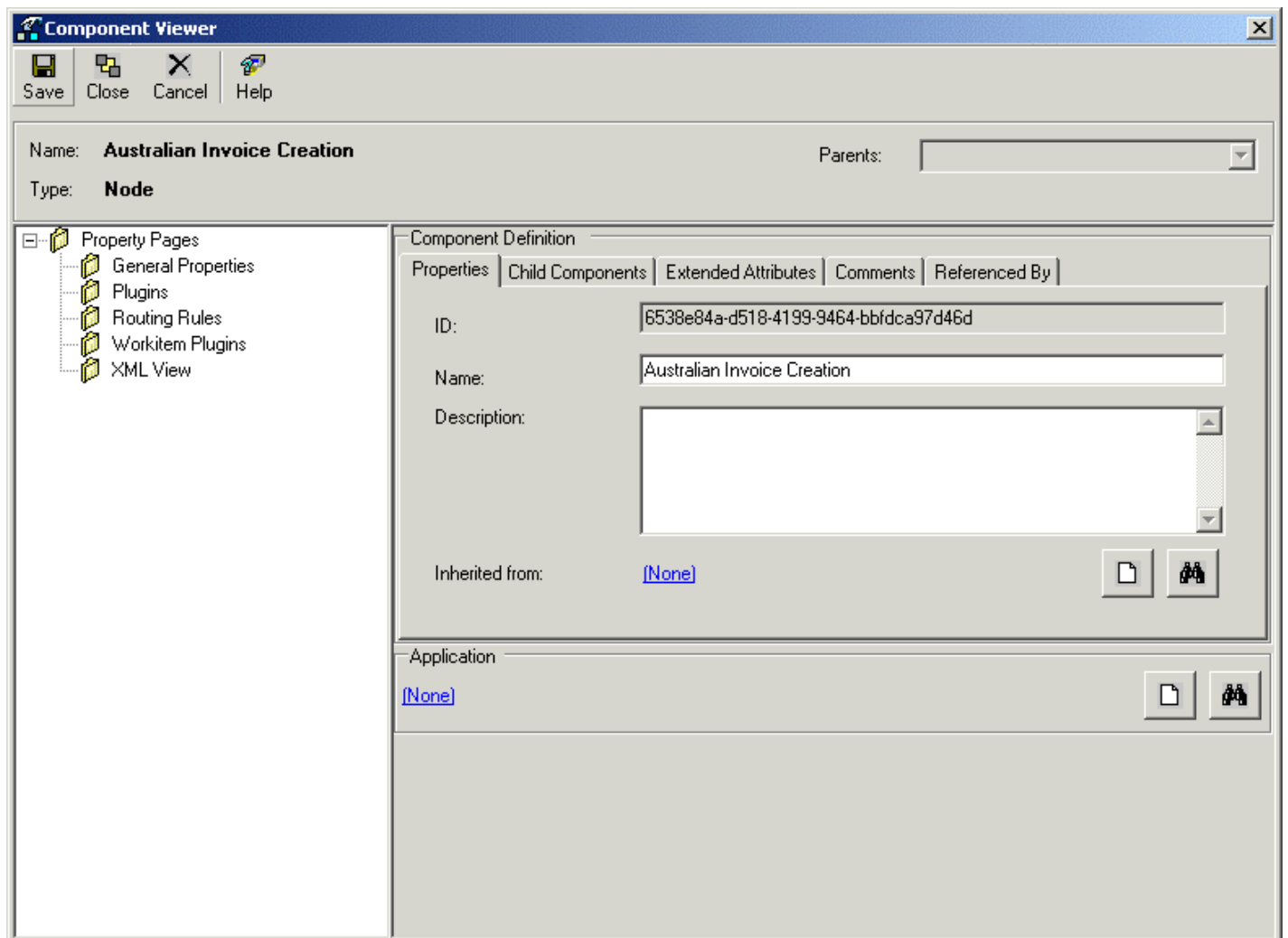


Figure 207: Specifying component properties

5. To define properties, in the left pane, select the appropriate property page.



The following table describes property pages:

Component property pages	
Name	Description
General Properties	Specifies general properties. If inheritance is used, allows selecting a parent component on which the new child component is based.
Dictionary	Specifies a custom user interface in Component Configuration Manager.
Plugins	Adds, modifies, and removes plugins.
Document Plugins	Adds and creates the following plugins: <ul style="list-style-type: none"> document filter document creation
Document Types	Adds, removes, and modifies document types.
Script Implementation	Specifies the interaction script.
Implementations	Defines the Java class, DLL entry point, executable file, or other implementation for a plugin.
Routing Rules	Specifies the following plugin types: <ul style="list-style-type: none"> entry routing rule exit routing rule
Workitem Plugins	Specifies the following plugin types: <ul style="list-style-type: none"> parallel work item rendezvous work item workitem prioritization
XML View	Displays the component's automatically generated XML definition. The definition is read-only.

6. To define general properties, in the **General Properties** page, select the appropriate tab and enter the required values.

The following table describes the **General Properties** page:

General Properties page		
Tab	Item	Description
Properties	ID	Unique component ID. This is assigned automatically and cannot be changed.
	Name	Component name.
	Description	Component description. This is optional.
	Inherited From	Parent component. If None appears, the component is not based on a parent component.

General Properties page		
Tab	Item	Description
		Adds a new component.
		Selects a parent component on which to base the child component.
Child Components		Child components of the currently selected component.
Extended Attributes		Node-specific custom properties that can be used by applications.
	Add	Adds an extended attribute.
	Modify	Modifies the selected extended attribute.
	Remove	Removes the selected extended attribute.
Comments		Attribute comments.
Referenced By		Components using the current component. This list describes the dependencies among components.

7. To define a dictionary, in the **Dictionary** page, proceed as follows:

- To specify the XML code that defines the user interface, in the right pane, perform one of the following steps:
 - Enter the XML code manually.
 - Copy XML code from the `ComponentDictionary.xml` template file, paste it into the pane, and edit the code as appropriate.

The `ComponentDictionary.xml` template file is located in the following directory:

```
\VisiFLOW\SYSTEM\CfgSchemas
```


For assistance with specifying the XML code, contact Exigen Professional Services.


- To save changes, click **Save**.
- To close the window, click **Close**.

8. To specify node plugins, proceed as follows:

- In the **Plugins** page, click **Add**.

The **Plugin** window appears.

- To use an existing plugin, click .
- Select the plugin.
- Click **Ok**.
- In the **Name** field, enter a plugin name.
- Click **Ok**.


- To add a new plugin, in the **Plugin** window, click .

The **Add New Component** window appears.


8. In the **Component Type** field, select a plugin type.
9. In the **Inherited From** field, optionally select a parent component.
10. In the **Component Name** field, enter the plugin name.
11. Click **Ok**.


The **Component Viewer** window appears.

12. In the **Component Viewer** window, define plugin properties.
13. To save changes, click **Save**.
14. To close the window, click **Close**.


15. To remove an existing plugin, in the **Plugin** window, click .





9. To define document plugins, in the **Document Plugins** page, proceed as follows:

- To add a new document filter plugin, in the **Document Filter Plugin** section, proceed as described in [Adding a New Component from a Component](#).
- To add an existing document filter plugin, in the **Document Filter Plugin** section, proceed as described in [Adding an Existing Component from a Component](#).
- To remove a document filter plugin, in the **Document Filter Plugin** section, click .
- To add a new document create plugin, in the **Document Create Plugin** section, proceed as described in [Adding a New Component from a Component](#).
- To add an existing document create plugin, in the **Document Create Plugin** section, proceed as described in [Adding an Existing Component from a Component](#).

- To remove a document create plugin, in the **Document Create Plugin** section, click .
10. To define document types for a configuration plugin, in the **Document Types** page, proceed as follows:
 - To add a document type, click **Add**, select the document type, and click **Ok**.
 - To remove a document type, select it and click **Remove**.


The **Modify** button is disabled to ensure that document types are not modified.

11. To define a script implementation, in the **Script Implementation** page, proceed as follows:
 - In the **Script Name** field, enter a script name.
 - In the **Project Name** field, enter a project.
 - In the **Project Path** field, enter a project path.
 - In the **Multi-Instance Subject Name** field, enter a multi-instance subject name.
12. To define an implementation for a plugin, in the **Implementations** window, in the **Java Class Name** field, enter a Java class name.
13. To define node routing rules, in the **Routing Rules** page, proceed as follows:
 - To add a new entry routing rule plugin, in the **Entry Routing Rule Plugin** section, proceed as described in [Adding a New Component from a Component](#).
 - To add an existing entry routing rule plugin, in the **Entry Routing Rule Plugin** section, proceed as described in [Adding an Existing Component from a Component](#).
 - To remove an entry routing rule plugin, click .

- To add a new exit routing rule plugin, in the **Exit Routing Rule Plugin** section, proceed as described in [Adding a New Component from a Component](#).
 - To add an existing exit routing rule plugin, in the **Exit Routing Rule Plugin** section, proceed as described in [Adding an Existing Component from a Component](#).
 - To remove an exit routing rule plugin, click .
14. To define workitem plugins for nodes, in the **Workitem Plugins** page, proceed as follows:
- To add a new parallel send workitem plugin, in the **Parallel Send Workitem Plugin** section, proceed as described in [Adding a New Component from a Component](#).
 - To add an existing parallel send workitem plugin, in the **Parallel Send Workitem Plugin** section, proceed as described in [Adding an Existing Component from a Component](#).
 - To remove a parallel send workitem plugin, click .
 - To add a new rendezvous workitem plugin, in the **Rendezvous Workitem Plugin** section, proceed as described in [Adding a New Component from a Component](#).
 - To add an existing rendezvous workitem plugin, in the **Rendezvous Workitem Plugin** section, proceed as described in [Adding an Existing Component from a Component](#).
 - To remove an existing rendezvous workitem plugin, click .
 - To add a new workitem prioritization plugin, in the **Workitem Prioritization Plugin** section, proceed as described in [Adding a New Component from a Component](#).
 - To add an existing workitem prioritization plugin, in the **Workitem Prioritization Plugin** section, proceed as described in [Adding an Existing Component from a Component](#).
 - To remove an existing workitem prioritization plugin, click .
15. To close the **Component Viewer** window without saving changes, click **Cancel**.
16. To save changes, click **Save**.
17. To close the window, click **Close**.

Adding a New Component from a Component

To add a new component from a component, proceed as follows:

1. In the appropriate component property page, click .
- The **Add New Component** window appears.
2. In the **Inherited From** field, optionally select a parent component.
 3. In the **Component Name** field, enter the new component name.
 4. Click **Ok**.


The **Component Viewer** window appears.

5. In the **Component Viewer** window, define properties as appropriate.

For information on defining component properties, following the instructions as described in [Adding a New Component](#), starting with step 5.

Adding an Existing Component from a Component

To add an existing component from a component, proceed as follows:

1. In the appropriate property page of the component, click .

The **Select Component** window appears.

2. In the table, select a component.
3. To cancel the action, click **Cancel**.
4. To save changes and close the window, click **Ok**.

Adding an Inherited Component

An inherited component is a child component based on an existing parent component.

To add an inherited component, proceed as follows:

1. In the **Component Configuration Manager** left pane, select the type or subtype of the parent component.

The components matching the selected type or subtype appear in the right pane.

2. In the right pane, select the parent component.
3. Click **Inherit**.

The **Add Inherited Component** window appears.

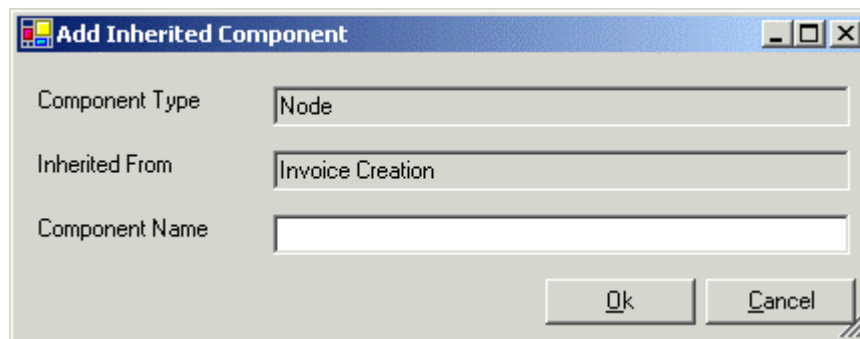


Figure 208: Adding an inherited component

4. In the **Component Name** field, enter a component name.
5. Click **Ok**.

The **Component Viewer** appears. It displays the name of the child component and properties defined for the parent component.

6. To modify inherited properties, in the left pane, select the property page.

In the right pane, a check box appears next to defined properties.

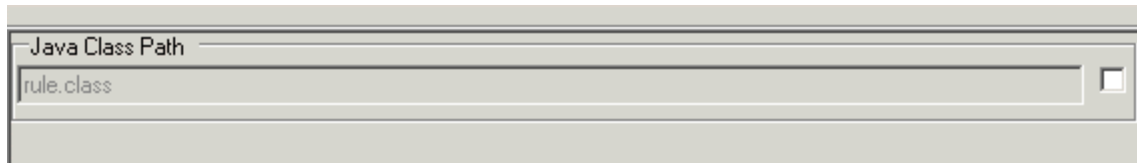



Figure 209: Inherited property

7. To modify an inherited property, select the check box and modify the property.
8. To cancel the changes, click **Cancel**.
9. To save changes, click **Save**.
10. To close the window, click **Close**.

As an alternative, a parent component can be assigned while adding a new component.

To assign a parent component while adding a new component, proceed as follows:

1. Start creating a new component as described in [Adding a New Component](#), steps 1 through 4.
2. To select a parent component, in the **General Properties** page, select the **Properties** tab, and click .
3. In the **Select Component** window, select a component.
4. To save the selection and close the window, click **Ok**.
5. To modify values inherited from the parent component, select the appropriate property page.
6. To modify an inherited property, select the check box and modify the property.
7. To cancel the changes, click **Cancel**.
8. To save changes, click **Save**.
9. To close the window, click **Close**.

Removing a Component

To remove a component, proceed as follows:

1. In the **Component Configuration Manager** window left pane, select the appropriate component type or subtype.

The components matching the selected type or subtype appear in the right pane.

2. In the right pane, select the component.
3. Click **Remove**.

A confirmation window appears.

4. To confirm the action, click **Yes**.
5. To cancel the action, click **No**.

Exporting Component Configurations

Component Configuration Manager exports component configurations to XML files.

To export component configurations using Component Configuration Manager, proceed as follows:

1. To open the **Import/Export** window, perform one of the following steps:
 - In the **Component Configuration Manager** window, select **File > Deploy Components**.
 - At the command line, enter the following:

```
menuccm.exe -d
```

The **Import/Export - Deployment Options** window appears.

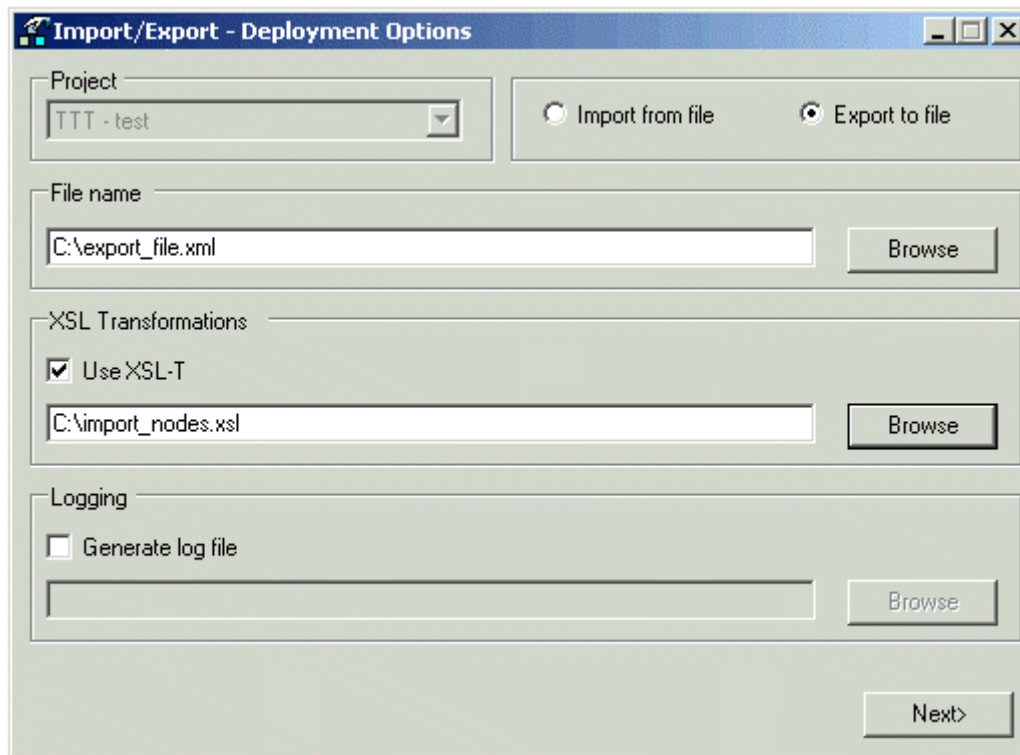


Figure 210: Exporting component configurations

2. If the window is opened using the command line, in the **Project** field, select a project from which component configurations are exported.

If the window is opened from the **Component Configuration Manager** window, the current project is selected and cannot be modified.

3. Select **Export to file**.

Component configurations can be exported as follows:

- by creating an XML file
- by overwriting an existing XML file
- by appending component configurations to an existing XML file

4. To export component configurations to a new XML file, in the **File name** field, enter the file name and path.
5. To export component configurations to an existing XML file, proceed as follows:
 - Next to the **File name** field, click **Browse**.
 - Select the file.
 - Click **Open**.
6. To export the configuration in a different XML format, in the **XSL Transformations** section, perform the following steps:
 - Select the **Use XSL-T** check box.
 - In the field, select the XSL transformation script file.

The XSL script file must be customized according to customer requirements.

7. To generate a log file for the export process, proceed as follows:
 - Select **Generate log file**.
 - Under the **Generate log file** option, specify the log file name and path.
8. Click **Next**.

If the export file exists, a confirmation message appears.

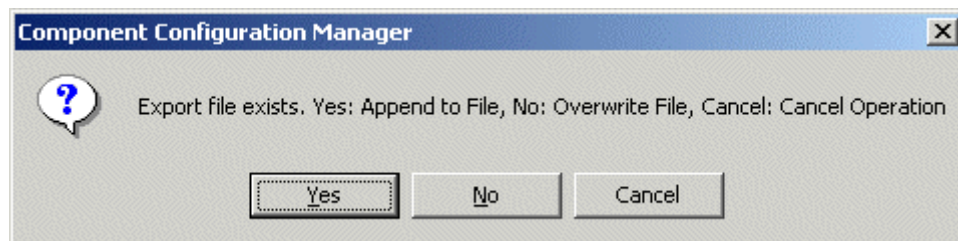


Figure 211: Confirming the export

9. To append the component configurations to the selected export file, click **Yes**.
10. To overwrite the selected export file, click **No**.
11. To cancel the export, click **Cancel**.

The **Import/Export - Selecting Components** window displays a component list.

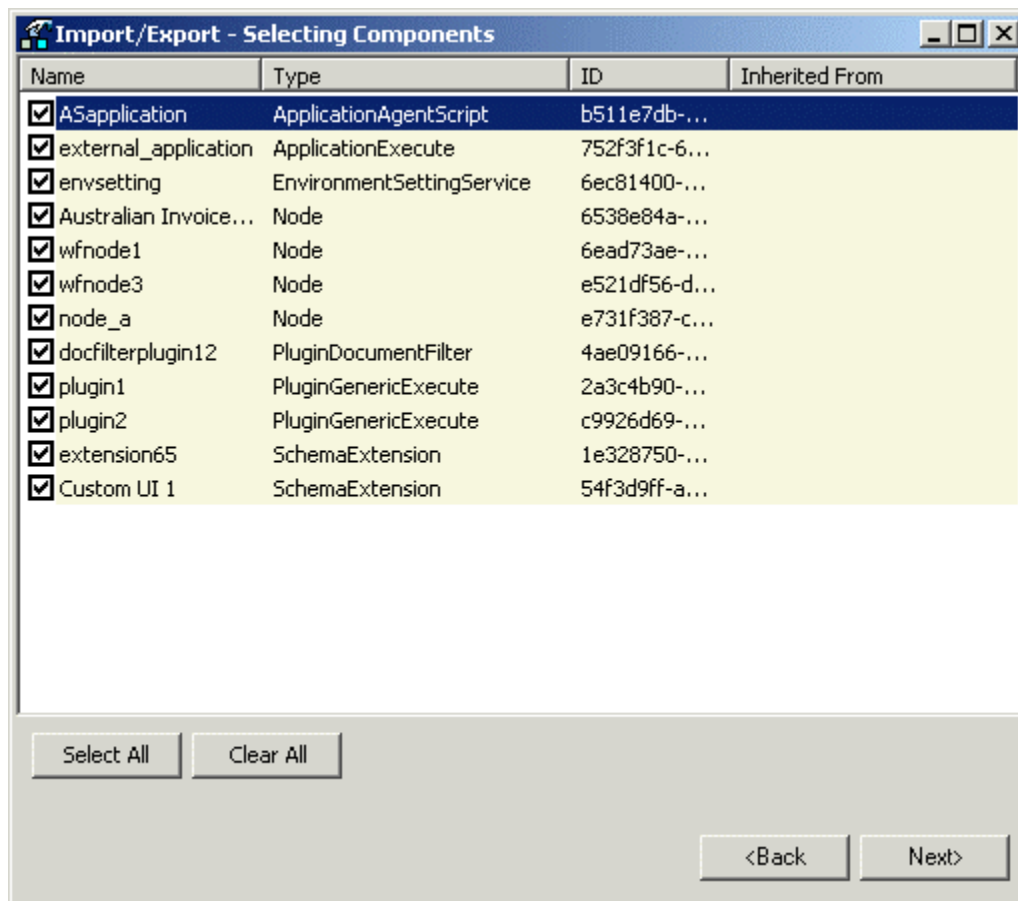


Figure 212: Selecting component configurations to export

12. Select the component configurations to export.
13. To select all component configurations, click **Select All**.
14. To deselect all component configurations, click **Clear All**.
15. Click **Next**.

If the export is to an existing file, the component configurations to be exported are compared with the component configurations in the existing file. In the **Action** column, new component configuration settings are designated as **New**. Identical component configuration settings are designated as **Identical**.

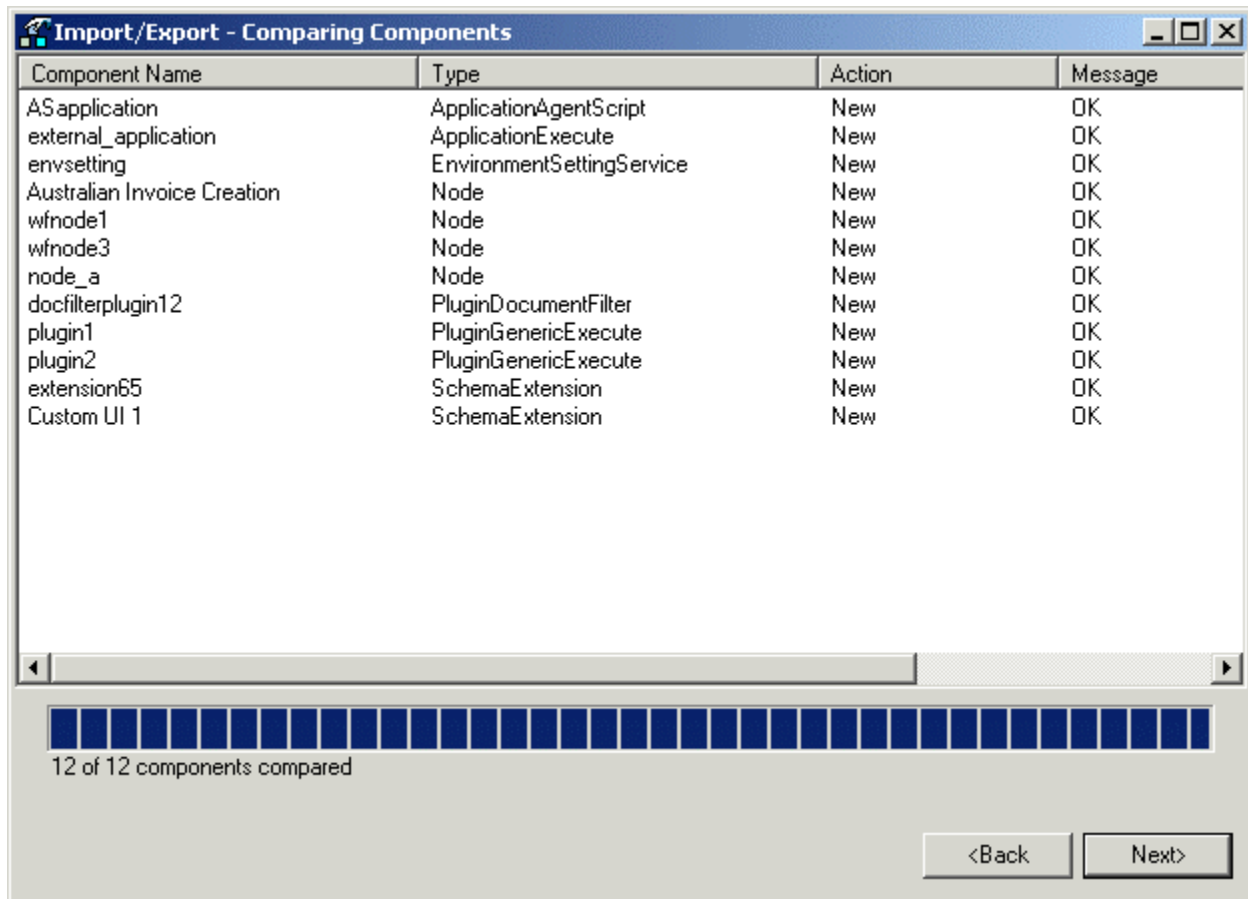


Figure 213: Comparing component configuration settings

16. To modify the component configurations to be exported, proceed as follows:

- Click **Back**.
- Modify the selection.
- Click **Next**.

17. To deploy the component configurations to the target file, click **Next**.

In the lower pane, the progress indicator displays the number of component configurations deployed.

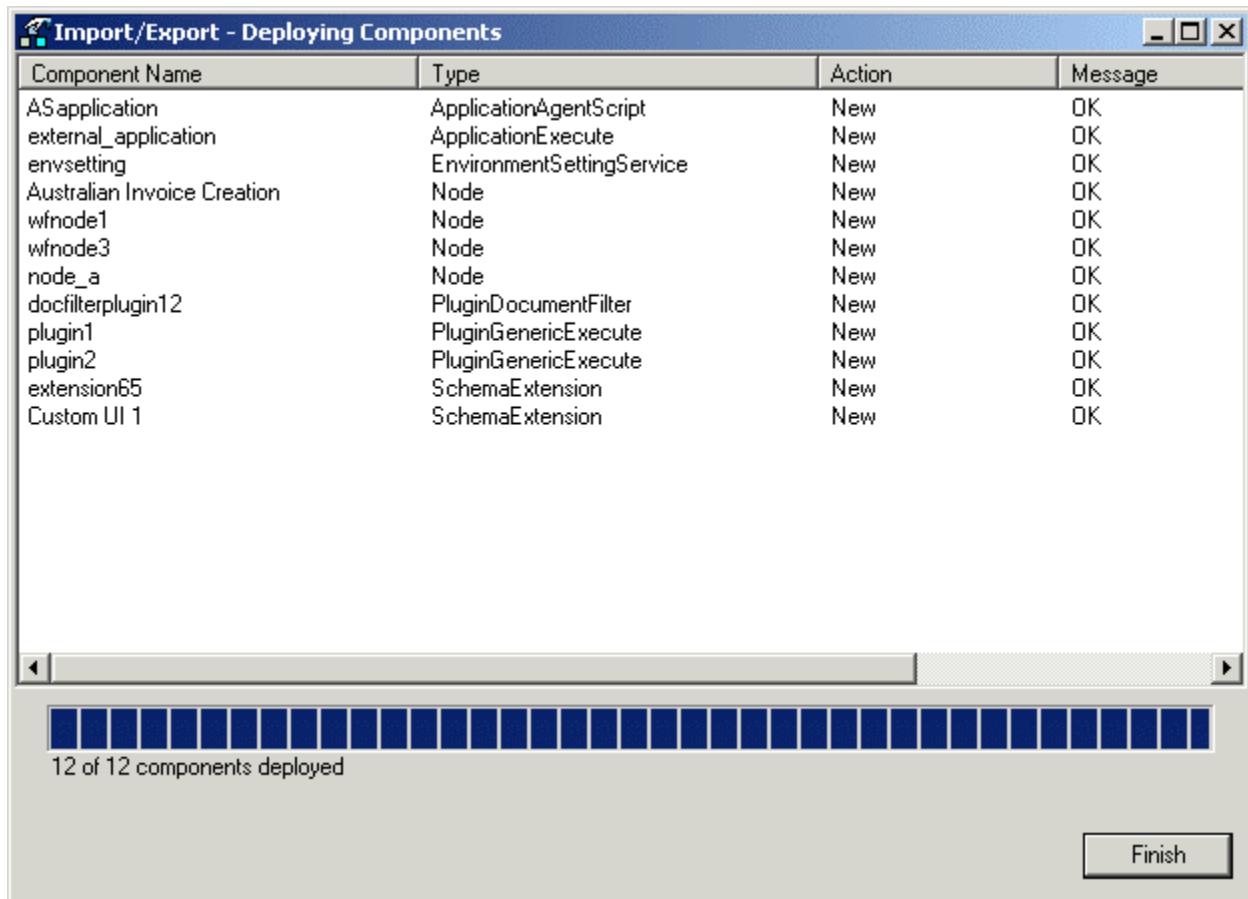


Figure 214: Deploying component configurations

18. To complete the process, click **Finish**.

Importing Component Configurations

Component configurations that are exported to an XML file can be imported into Component Configuration Manager.

To import component configurations into Component Configuration Manager, proceed as follows:

- To open the **Import/Export** window, perform one of the following steps:
 - In the **Component Configuration Manager** window, select **File > Deploy Components**.
 - At the command line, enter the following:

```
menuccm.exe -d
```

The **Import/Export - Deployment Options** window appears.

- If the window is opened using the command line, in the **Project** field, select a project to which settings are imported.

If the window is opened from the **Component Configuration Manager** window, configuration settings are imported to the current project.

3. Select **Import from file**.
4. In the **File name** field, enter the path and file name to be imported, or to select the file, click **Browse**.

Only XML files can be imported.

5. To import the configuration from a different XML format, in the **XSL Transformations** section, perform the following steps:
 - Select the **Use XSL-T** check box.
 - In the field, select the XSL transformation script file.

The XSL script file must be customized according to customer requirements.

6. To generate a log file for the import process, proceed as follows:
 - Select **Generate log file**.
 - Under the **Generate log file** option, specify the log file name and path.
7. Click **Next**.

The list of component configurations in the selected XML file are displayed.

8. Select the component configurations to import.
9. To select all components, click **Select All**.
10. To deselect all components, click **Clear All**.
11. Click **Next**.

If discrepancies are detected, error or warning messages are displayed.

Discrepancies are detected in the following cases:

- A component configuration is selected for a workflow or node that does not exist in the destination project.
- A component configuration is selected for a workflow or node that exists in the destination project, but has a different ID. In this case, a warning indicates that the component configuration is imported with its original IDs.

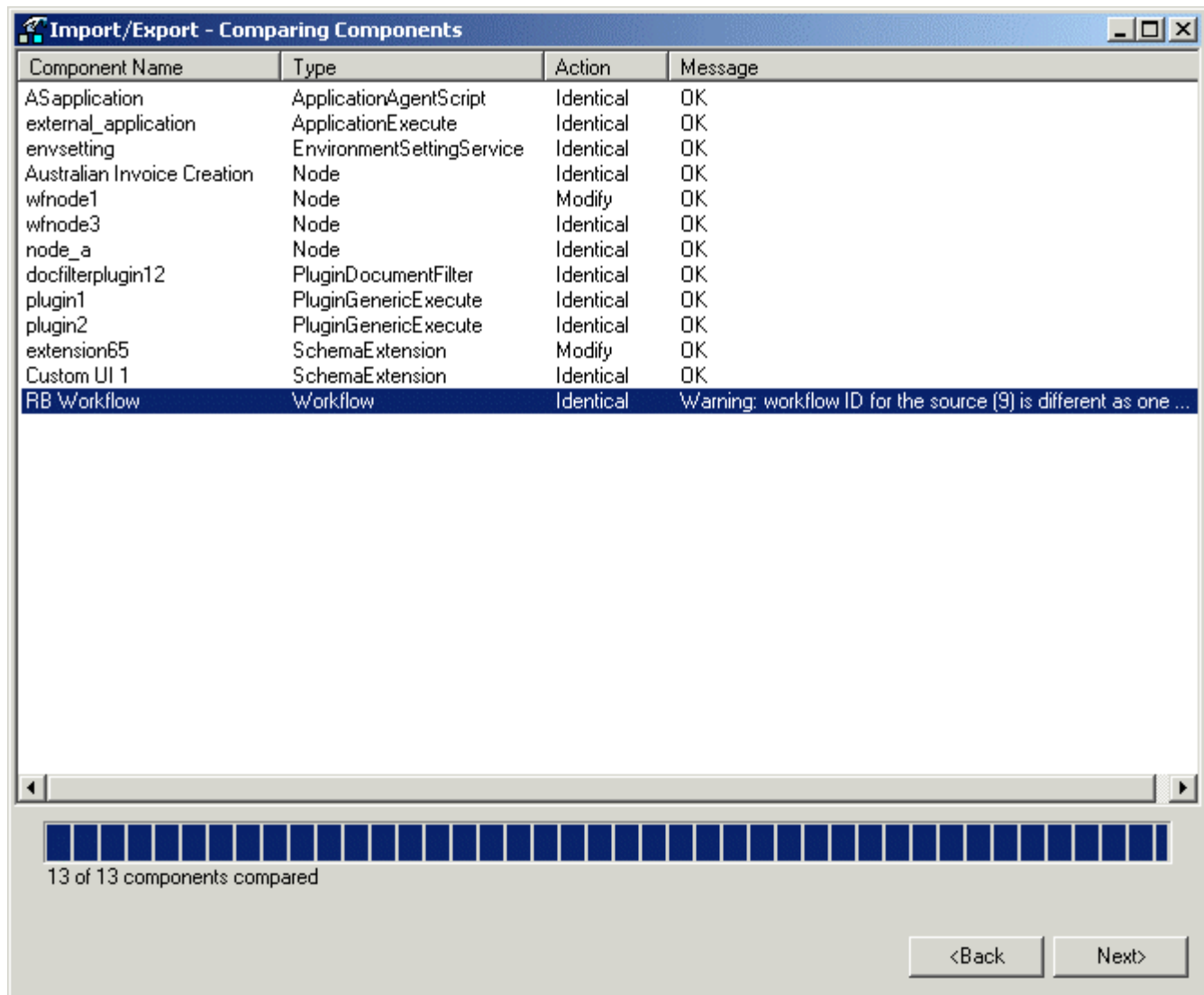


Figure 215: Viewing error messages

12. To correct errors, proceed as follows:

- Click **Back**.
- Clear the components that are causing errors.
- Click **Next**.

13. To import the selected component configurations to the target database, click **Next**.

In the lower pane of the **Import/Export** window, the progress indicator shows how many component configurations are imported.

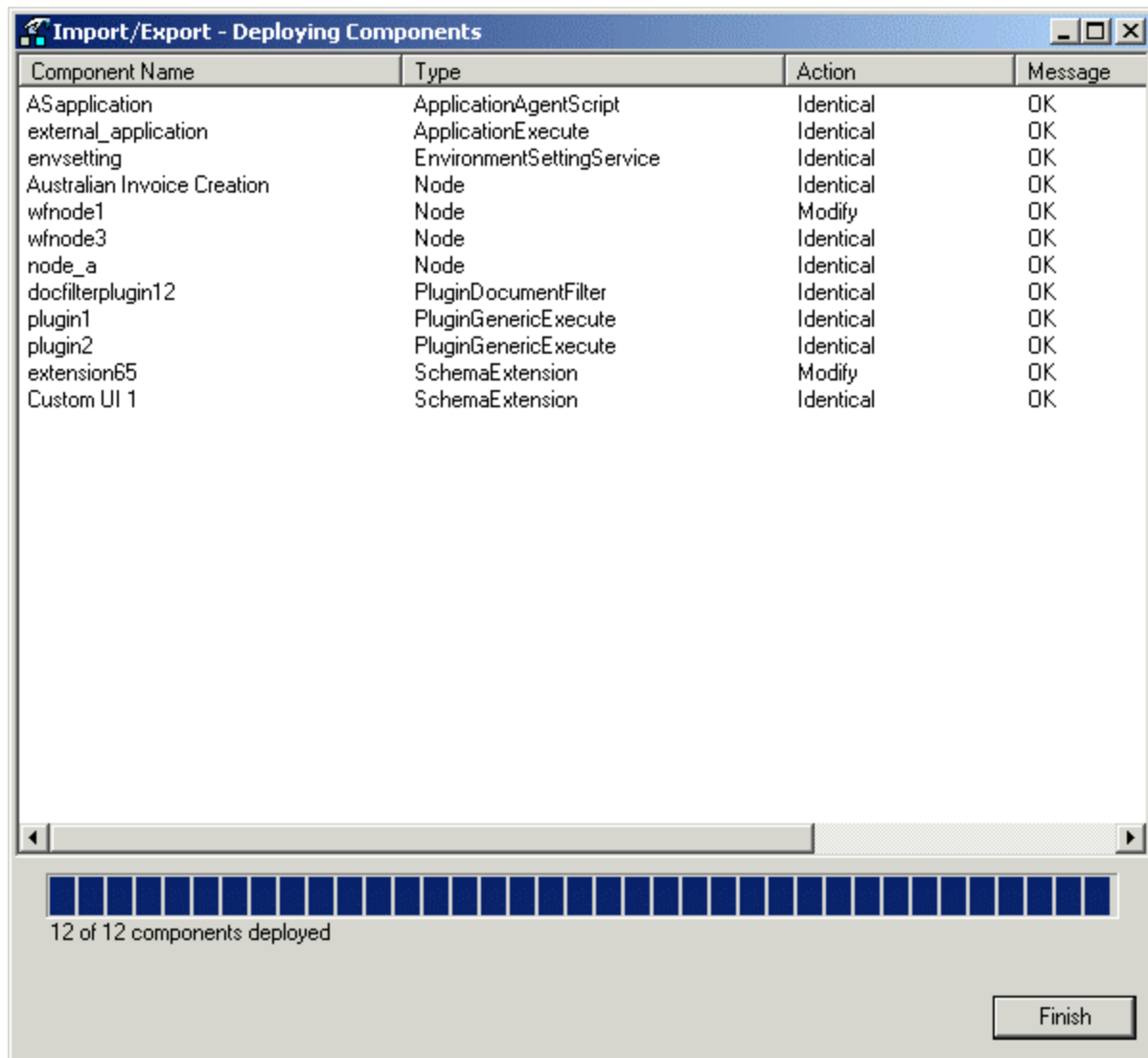


Figure 216: Completing the import process

14. To complete the import process, click **Finish**.

Viewing and Modifying a Component

To view and modify an existing component, proceed as follows:

1. In the **Component Configuration Manager** window left pane, select the appropriate component type or subtype.

The components matching the selected type or subtype appear in the right pane.

2. To view component properties, in the right pane, double click a component.

The **Component Viewer** window displays component properties.




3. In the left pane, select the property page to be modified.

The property page appears in the right pane.

4. In the right pane, modify the properties as required.
5. To cancel the changes, click **Cancel**.
6. To save the changes, click **Save**.
7. To close the window, click **Close**.

Component Configuration Manager Window Buttons and Menu Commands

The **Component Configuration Manager** window includes the following buttons and menu commands:

Component Configuration Manager window buttons and menu commands		
Button	Menu command	Description
	File > Load New Schema	Load New Schema Imports a schema and a component dictionary into the database.
	File > Exit	Exit Exits Component Configuration Manager.
	File > Deploy Components	Deploy Components Imports and exports component configurations.
	Component > Add	Add Adds a component.
	Component > Remove	Remove Removes the selected component.
	Component > Inherit	Inherit Creates a child component that inherits properties from the selected parent component.
	Help > About	About Displays information on the current Exigen Workflow version.

Chapter 6: Managing the Workflow

This chapter discusses how to monitor and maintain workloads within the workflow. The following topics are described in this section:





- [Overview](#)
- [Graphical Queues Workload Monitor Window](#)
- [Graphical Users Workload Monitor Window](#)
- [Workload Distribution Monitor Window](#)
- [Dealing with Problematic Documents](#)
- [Using Document Versioning](#)

Overview

The **Workflow Monitor** tool monitors workloads within the queues and redistributes them if required.

If ACL based security is implemented, only users and user groups with the required permissions can view documents and folders in Workflow Monitor. For information on assigning permissions to users and user groups, see [Security Tab](#).

Workflow Monitor consists of the following tools:

Workflow Monitor tools		
Tool	Button	Description
Graphical Queues Workload Monitor		Workload distribution by queue.
Graphical Users Workload Monitor		Workload distribution by user.
Workload Distribution Monitor		Lists of workloads as a result of queries based on node and user.
Work Item Notes		Lists of jobs sent to the administrator via the Retrieve object.

Workflow Monitor is located in the **Workflow Tools** folder in **Administration Tools** in Exigen Workflow Explorer.

To use **Workflow Monitor**, proceed as follows:

1. Click the **Workflow Monitor** icon.



The **Workflow Monitor** window appears.

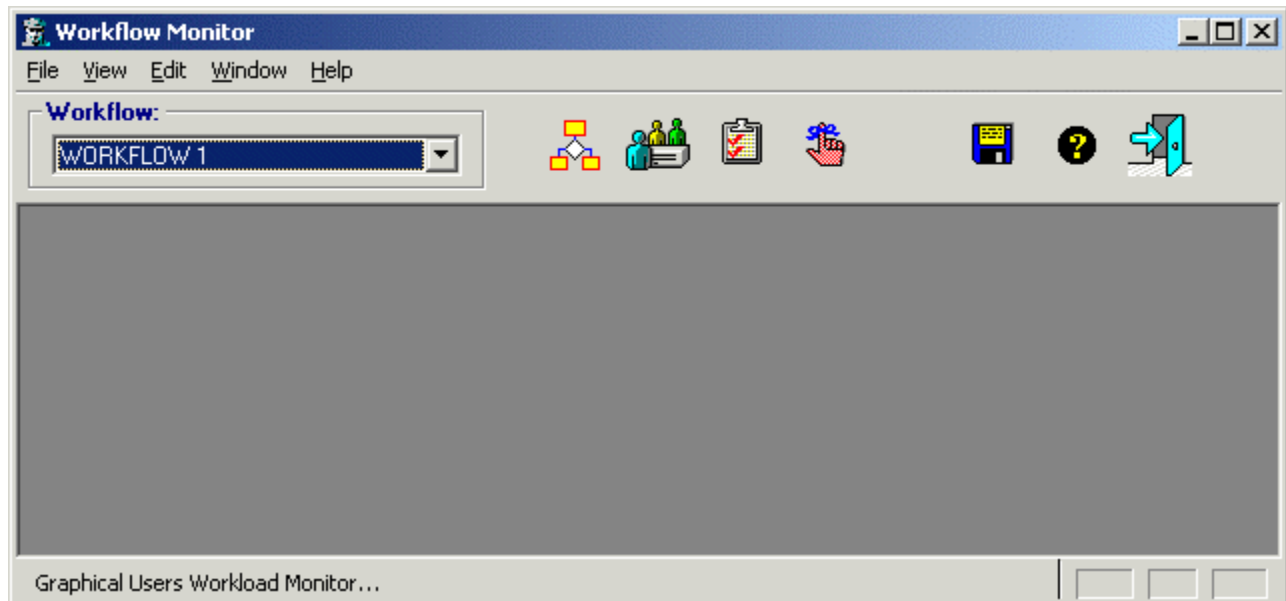


Figure 217: Workflow Monitor window

2. In the **Workflow** list, select the workflow application to be monitored.
3. To open a Workflow Monitor tool, click the appropriate button.

For more information on Workflow Monitor tools, see [Graphical Queues Workload Monitor Window](#), [Graphical Users Workload Monitor Window](#), [Workload Distribution Monitor Window](#), and [Dealing with Problematic Documents](#).

4. To ensure that the **Workflow Monitor** window is displayed at the same position next time it is opened, click **Save Configuration**.



5. To close the **Workflow Monitor** window, click **Exit**.



Graphical Queues Workload Monitor Window

The **Graphical Queues Workload Monitor** window displays a graphical representation of the jobs existing in each queue or node. The graphs can be displayed as two or three-dimensional graphs.

To view the queue graphs, proceed as follows:

1. Click **Graphical Queues Workload Monitor**.



The **Graphical Queues Workload Monitor** window appears.

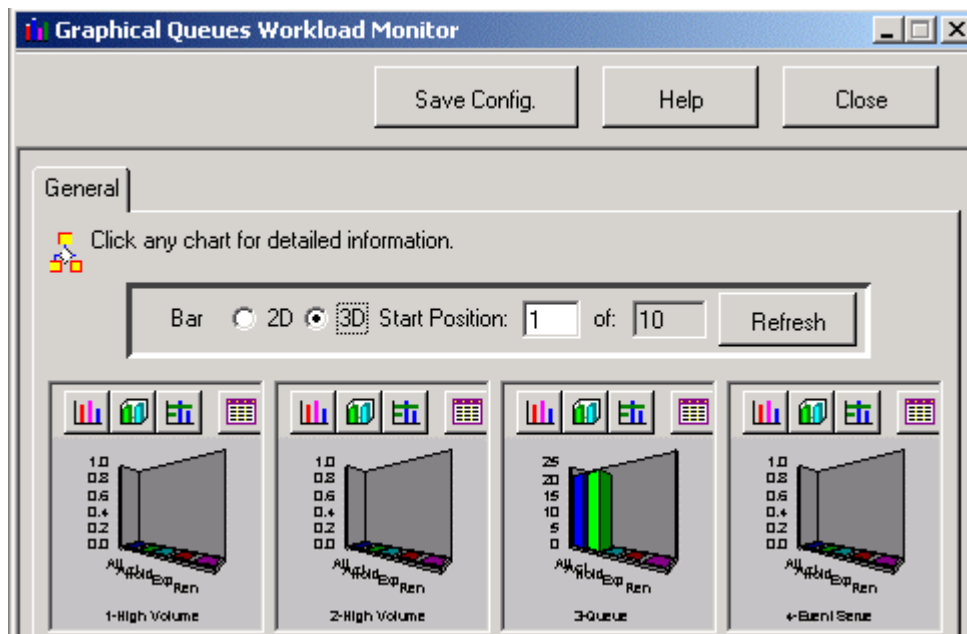


Figure 218: Graphical Queues Workload Monitor window

The visual presentation of the graphs can be changed by clicking the buttons above each graph.

2. To see the current presentation, click **Refresh**.

Graphical Users Workload Monitor Window

The **Graphical Users Workload Monitor** window displays a graphical representation of the jobs for each user. It is similar to the **Graphical Queues Workload Monitor** window.

To view the user graphs, proceed as follows:

1. To open the **Graphical Queues Workload Monitor** window, click **Graphical Queues Workload Monitor**.



The **Graphical Users Workload Monitor** window appears.

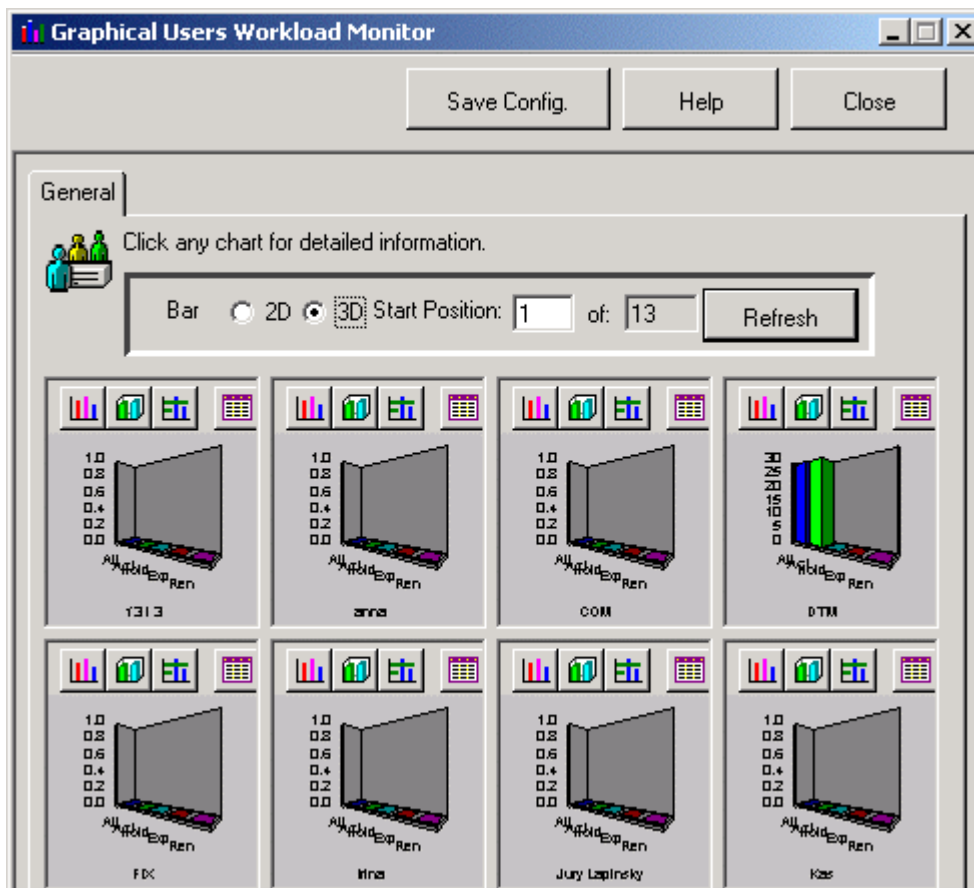


Figure 219: Graphical Users Workload Monitor window

The visual presentation of the graphs can be changed by clicking the buttons above each graph.

2. To see the current presentation, click **Refresh**.

Workload Distribution Monitor Window

The **Workload Distribution Monitor** window shows detailed listings of the jobs in each queue. The lists can be displayed for one or all queues, or one or more users. Jobs can be moved from one queue to another to balance workloads. Totals for each queue and user can be generated.

To view these listings, click **Workload Distribution Monitor**.



The **Workload Distribution Monitor** window appears.

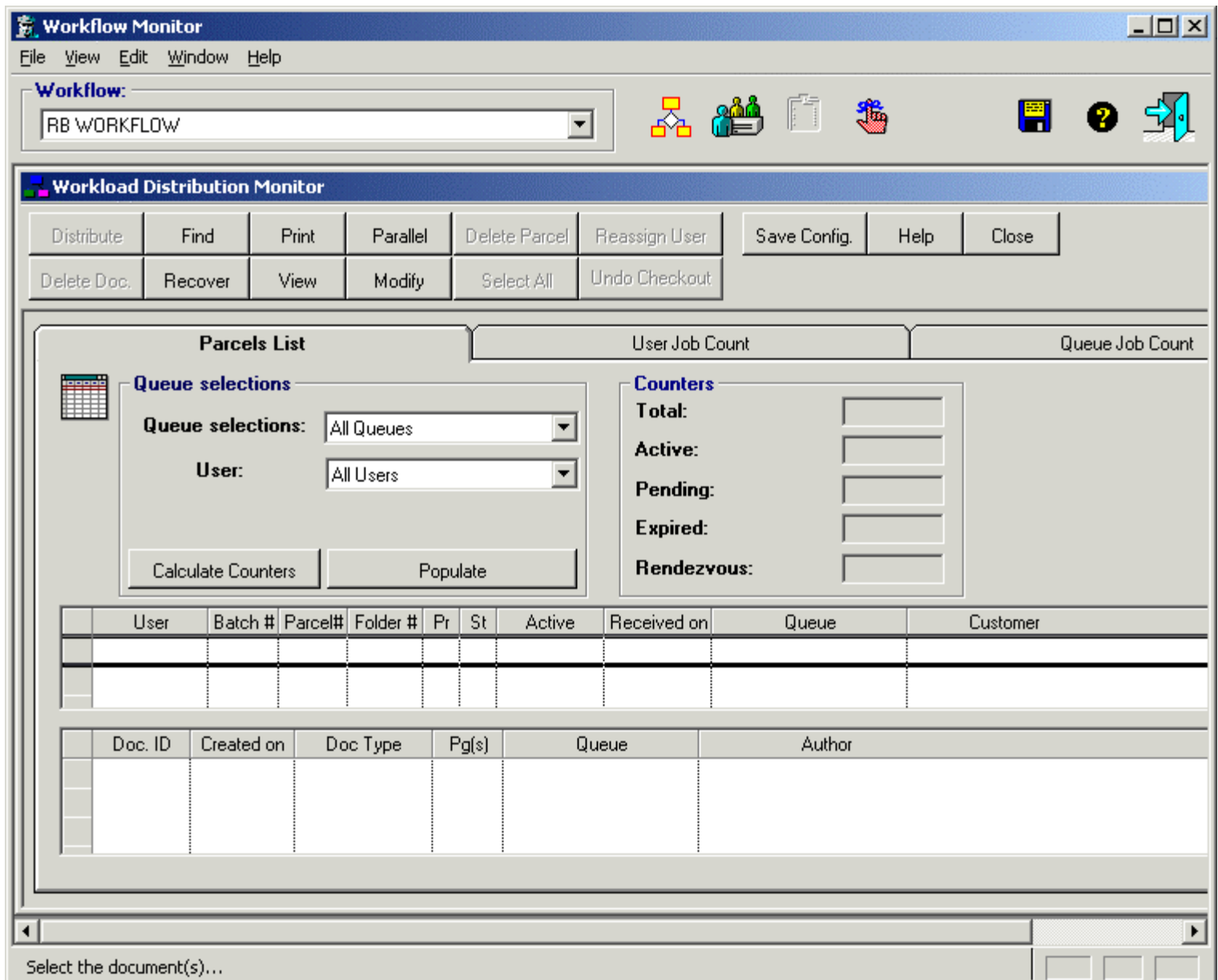


Figure 220: Workload Distribution Monitor window

The following topics are described in this section:

- [Viewing, Distributing, Reassigning, and Printing Parcels](#)
- [Resetting Parcel Times](#)
- [Configuring Node and User Display Settings](#)
- [Deleting Parcels](#)
- [Viewing User Job Statistics](#)
- [Viewing Queue Job Statistics](#)
- [Understanding the Workload Distribution Monitor Window](#)

Viewing, Distributing, Reassigning, and Printing Parcels

The **Parcels List** tab is used to display detailed listings of the jobs or parcels in the queues for one or all users. To see current data, proceed as follows:

1. In the **Queue selections** list, select one or all queues.
2. In the **User** list, select one or all users.

The lists of available queues and users depend on the node and user display settings. For information on configuring node and user display settings, see [Configuring Node and User Display Settings](#).

3. To display the number of parcels in the workflow, click **Calculate Counters**.

The following information appears in the **Counters** section of the window:

Calculate Counters section	
Name	Description
Total	All parcels.
Active	Parcels with active status.
Pending	Parcels on hold.
Expired	Overdue parcels.
Rendezvous	Parcels waiting to be reunited with parallel parcels in a specified rendezvous queue.

If the number of parcels is large, additional search values can be specified.

4. To see the list of parcels corresponding to your query, click **Populate**.
5. To display the documents in the bottom table, double click on a parcel in the top table.

The columns displayed represent selected fields when the project was created with **Project Builder**. Also displayed are the custom table fields.

For more information on the **Parcels List** tab, see [Workload Distribution Monitor Parcels List Tab](#).

For information on monitoring tasks, see the *Task Oriented Workflow Administrator's Guide*, Chapter 6: Monitoring Tasks.

Sorting Parcels Using the Sort Function

To sort parcels using the Sort function, proceed as follows:

1. To open the Sort window, in the parcels area, point and right-click. Select **Sort**.

The **Sort** window appears.

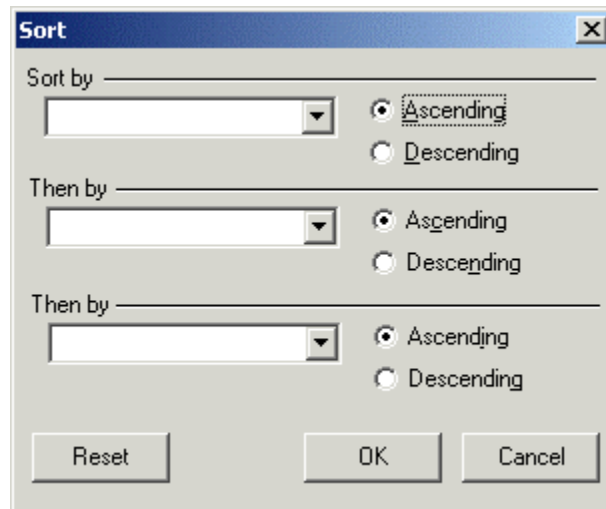


Figure 221: Sort window

6. Select the field to sort by.

The **Sort By** and **Then By** submenus list all fields that are displayed in the parcel table. The parcels are sorted first by **Sort By** values and then by **Then By** values.

7. To change the sort order, click either **Ascending** or **Descending**.
8. To revert to the default sort order, select **Reset**.
9. To save a sort setting, select **File > Save Configuration**.

Distributing Parcels

To distribute work to another queue and user, proceed as follows:

1. To select a parcel for distribution, click it.
2. To select several parcels for distribution, press **CTRL** and click the parcels.
3. To select all parcels for distribution, click **Select All**.
4. Click **Distribute**.

The **Distribute Parcels** window appears.

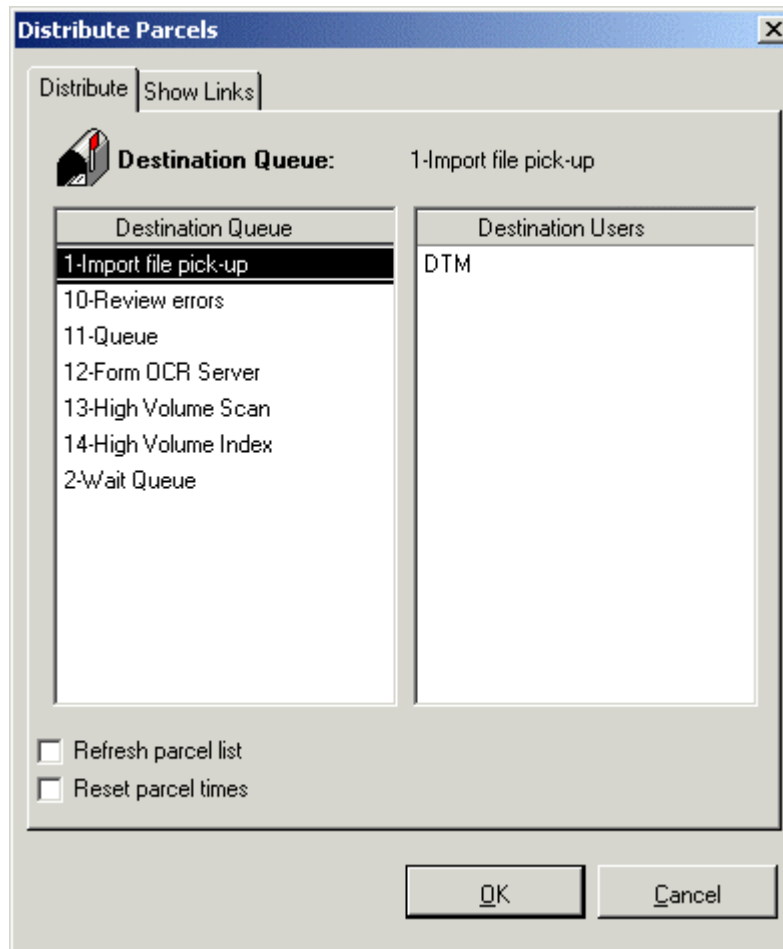


Figure 222: Distribute Parcels window

5. Select the queue and the user to which you want to send the parcels.
6. To repopulate the parcel list automatically, select the **Refresh parcel list** check box.
7. To reset parcel times, select the **Reset parcel times** check box.

For information on resetting parcel times, see [Resetting Parcel Times](#).

8. Click **OK**.

Reassigning a Parcel

To reassign a parcel to another user for processing, proceed as follows:

1. To select a parcel, click it.
2. To select several parcels, press **CTRL** and click the parcels.
3. To select all parcels, click **Select All**.
4. Click **Reassign User**.

The **Reassign User** window appears.



Figure 223: Reassign User window

5. Select the user to whom you want to send the parcels.
6. To repopulate the parcel list automatically, select the **Refresh parcel list** check box.
7. To reset parcel times, select the **Reset parcel times** check box.

For information on resetting parcel times, see [Resetting Parcel Times](#).

8. Click **OK**.

Printing a Report

A brief report is one that covers no more than 10 database fields. To specify printing options and print a brief report about the parcel, proceed as follows.

1. In the **Workload Distribution Monitor** window, select the parcel and click **Print**.

The **Print Batch/Parcel List** window appears.

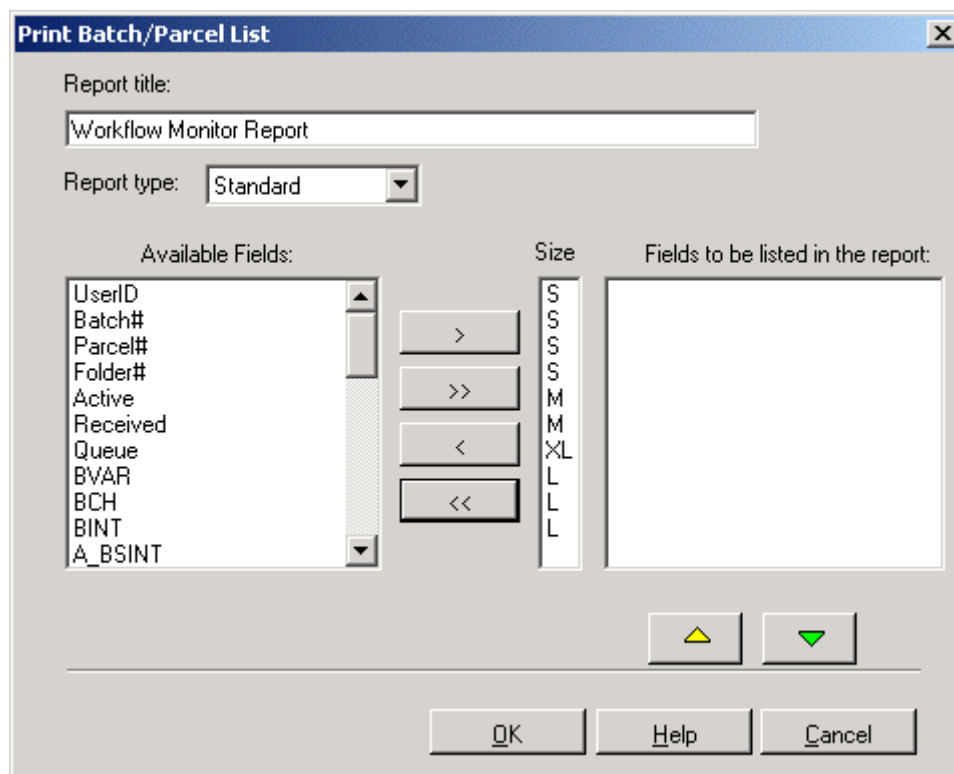


Figure 224: Print Batch/Parcel List window

2. In the **Report title** field, enter a report title.
3. In the **Report type** field, select one of the following report types:

Report types	
Name	Description
Standard	Report with the selected database fields appears in the Centura Report Builder window, where it can be viewed and printed.
Excel	Report appears in XLS format in the <code>repmonitoring.xls</code> file in the Exigen Workflow system directory.

If you are creating an Excel report for the first time, the template file `repmonitoring_template.xlt` appears.

4. To specify the fields included in the report, in the **Available Fields** list, select a field and click the right arrow **>**.
5. To move all fields to the **Fields listed in the report** list, click the double right arrow **>>**.
6. For the **Standard** report type, specify the size of the respective field:

Field sizes	
Name	Description
S	Small
M	Medium
L	Large

Field sizes	
Name	Description
XL	Extra large

As the letter arrangement stays constant, click the up and down arrow buttons to match a field with the size of the cell in which it is printed.

7. As the fields are different lengths, it is recommended that you match the field size with the size of the report table cell.

8. Click **OK**.

The report is printed.

Resetting Parcel Times

The **Reset parcel times** option automatically resets the parcel time to the current date and time when a parcel is distributed or reassigned to a different user.

To enable the reset parcel times option, proceed as follows:

1. Start Configuration Browser.

For information on starting Configuration Browser, see [Starting Configuration Browser](#).

2. In the left pane, locate the `WFMonitor` section.
3. If the `WFMonitor` section does not exist, add a `WFMonitor` section for the appropriate user and workflow.

For information on adding a configuration section, see [Adding a Configuration Section](#).

4. To ensure that the **Reset parcel times** check box is enabled, in the right pane, right click `Workflow Monitor` and select **Add > ChangeResetTimesSettings**.
5. Set the **ChangeResetTimesSettings** value to **Yes**.
6. Click **Apply**.

By default, parcel times are not reset automatically.

7. To specify that parcel times are reset by default, in the right pane, right click `Workflow Monitor` and select **Add > ResetParcelTimes**.
8. Set **ResetParcelTimes** to **Yes**.
9. Click **Apply**.
10. Close Configuration Browser.

11. To reset the parcel time when distributing a parcel, in the **Distribute Parcels** window, select the **Reset parcel times** check box.

For information on distributing parcels, see [Distributing Parcels](#).

12. To reset the parcel time when reassigning a parcel, in the **Reassign User** window, select the **Reset parcel times** check box.

For information on reassigning a parcel, see [Reassigning a Parcel](#).

Configuring Node and User Display Settings

To configure the node and user display settings, proceed as follows:

1. In the **Workflow Monitor** window, select **File > Node/User Selection Settings**.

The **Node/User Selection Settings** window appears.

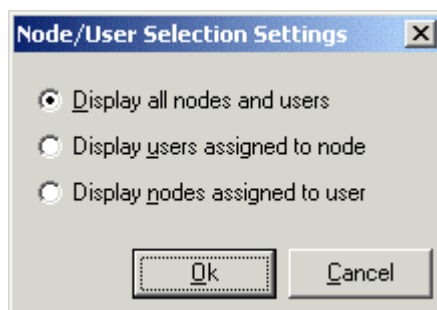


Figure 225: Node/User Selection Settings window

2. In the **Node/User Selection Settings** window, select one of the following options:

Node/User Selection Settings window options	
Option	Description
Display all nodes and users	In the Workload Distribution Monitor window, all nodes and users can be selected for monitoring.
Display users assigned to node	In the Workload Distribution Monitor window, if a node is selected, only the users having access to the node are available for selection.
Display nodes assigned to user	In the Workload Distribution Monitor window, if a user is selected, only the nodes that the user has access to are available for selection.

3. To save the changes, click **Ok**.

To prevent a user from changing job count hour column settings, in the **WFMonitor** section of Configuration Browser, set *No* for the item **ChangeWorkdaySettings**. For information on creating configuration sections in Configuration Browser, see [Adding a Configuration Section](#).

Deleting Parcels

To delete a parcel, proceed as follows:

1. To view available parcels, in the **Workload Distribution Monitor** window, click **Populate**.
2. In the upper table, select a parcel to delete.
3. Click **Delete Parcel**.

The **Confirmation** window appears.

4. To confirm the deletion, click **Yes**.
5. To cancel the action, click **No**.

If you click **Yes**, and the parcel to be deleted is a parallel parcel, the **Delete Parallel Parcel** window appears.

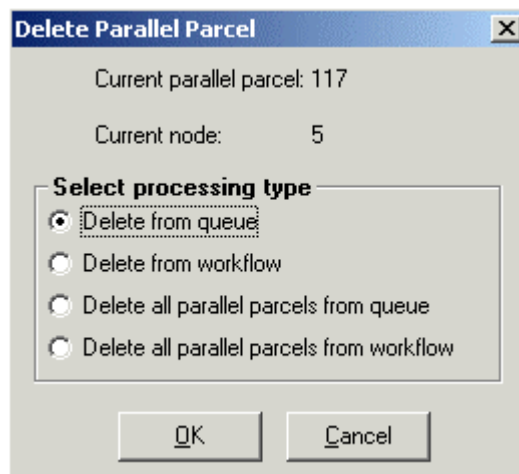


Figure 226: Deleting a parallel parcel

The **Delete Parallel Parcel** window displays the number of the selected parallel parcel and its node.

6. To specify which parallel parcels are to be deleted, in the **Select processing type** section, select one of the following options:

Parallel parcel delete options	
Name	Description
Delete from queue	Deletes the selected parcel from the queue.
Delete from workflow	Deletes all instances of the selected parallel parcel.
Delete all parallel parcels from queue	Deletes all instances of parallel parcels from the queue in which the selected parallel parcel is located.
Delete all parallel parcels from workflow	Deletes all parallel parcels from the workflow. Note: The project manager's permission is required before using this option.

7. To confirm the deletion, click **OK**.
8. To cancel the action, click **Cancel**.

Viewing User Job Statistics

The **User Job Count** tab displays the total number of jobs waiting for each user.

Parcels List **User Job Count** Queue Job Count

Queue Selections: 9-Scan Low

Show Users Show Selected Info Configure Hour Columns

User	Parcel	Active	Pending	Exp	Rend	1 h in queue	2 h in queue	3 h in queue	>3 h in queue
ART	1	1	0	0		0	0	0	1
DTM	2	2	0	0		0	0	0	2

Figure 227: User Jobs Count tab

To view user job statistics, proceed as follows:

1. In the **Queue selections** box, select **All Queues** to retrieve statistics for all queues, or select a specific queue.
2. To view all users of a selected queue, click **Show Users**.
3. In the table, select one or more users.
4. To view the number of jobs waiting for the selected users, click **Show Selected Info**.

The last columns display the number of jobs remaining in the queue for less than 1, 2, or 3 hours, or more than 3 hours. For example, the column **3 h in queue** shows parcels that were sent to the user more than 2 hours but less than or equal to 3 hours ago.

To configure job hours and column names, proceed as follows:

1. To exclude non-business days, use the ESC_CAL table.

For information on the ESC_CAL table, see the *Exigen Workflow Administrator's Guide, Part 2: Business Component Reference*, Chapter 11: Escalation Server and Log, Excluding Non-Business Days and Holidays.

2. Click **Configure Hour Columns**.

The **Configure Job Count Hour Columns** window appears.

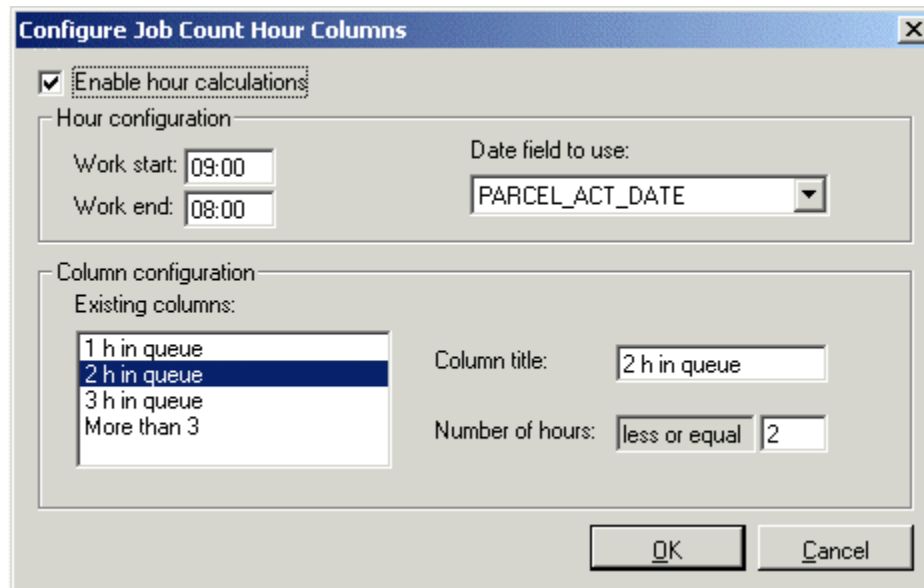


Figure 228: Configure Job Count Hour Columns window

3. To enable the calculation of hours, select **Enable hour calculations**.
4. In the **Hour configuration** box, modify when work starts and ends in your company by entering the start and end times in the **Work start** and **Work end** fields using the colon : as a delimiter.
5. In the **Date field to use** list box, select the BATCHPARCEL table date column that is used as a starting point to calculate the time the parcel spends in the queue.
6. To change a column name, select the column in the **Existing Columns** list and enter a new column name in the **Column Title** field.
7. To change the number of hours, select the column in the **Existing Columns** list and enter a new value in the **Number of Hours** field.

For example, you can create an hour column *Less than 12 h*. To do this, select one of the first three columns in the **Existing columns** list, change **Column title** to *Less than 12 h* and enter 12 in the **Number of Hours** field.

8. After changing the settings, click **OK**.

The changes are applied to the specific user in the workflow.

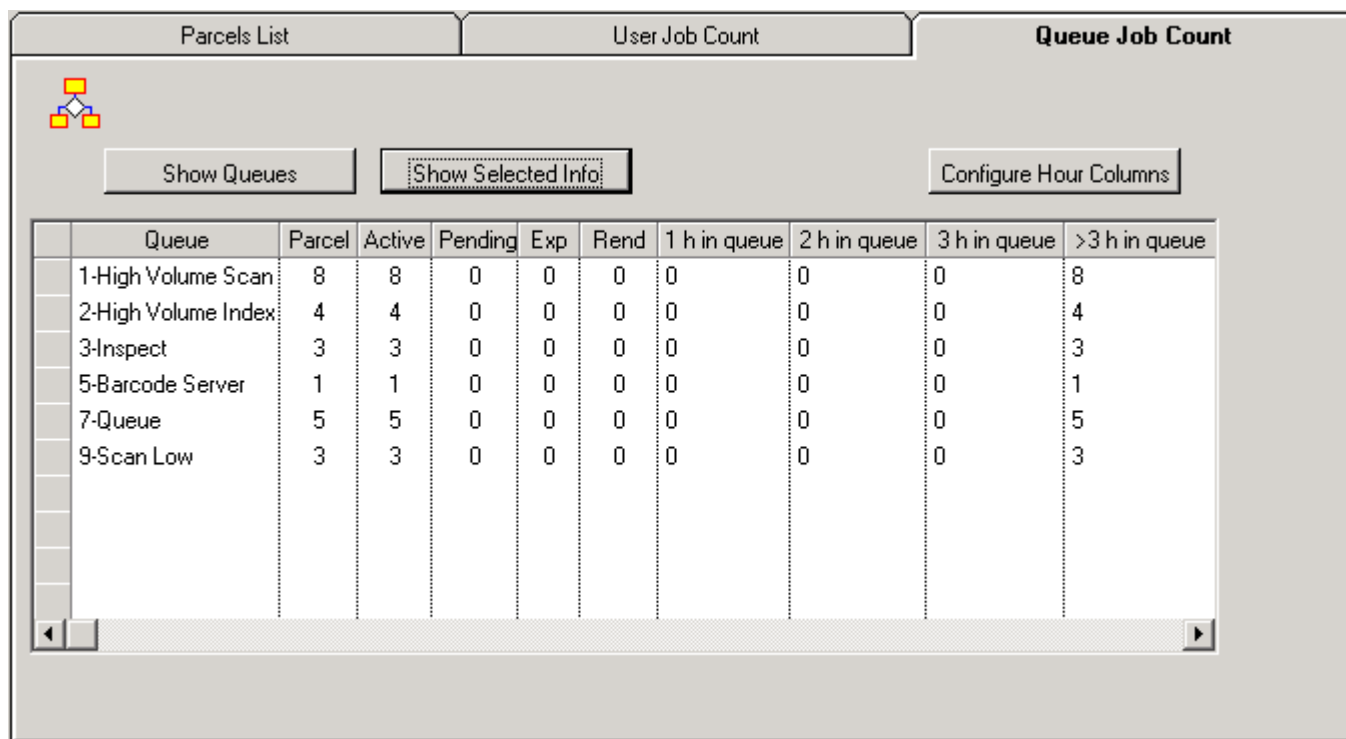
To prevent a user from changing job count hour column settings, set *No* for the item **ChangeWorkdaySettings** in the **WFMonitor** section of Configuration Browser. For information on creating configuration sections in Configuration Browser, see [Adding a Configuration Section](#).

Changes can be applied to all users in the workflow by using Configuration Browser to create a configuration section for the workflow. For information on applying changes to all users in the workflow, see [Adding a Configuration Section](#).

For more information on the **User Job Count** tab, see [Workload Distribution Monitor User Job Count Tab](#).

Viewing Queue Job Statistics

The **Queue Job Count** tab displays the total number of jobs available in each queue.



Queue	Parcel	Active	Pending	Exp	Rend	1 h in queue	2 h in queue	3 h in queue	>3 h in queue
1-High Volume Scan	8	8	0	0	0	0	0	0	8
2-High Volume Index	4	4	0	0	0	0	0	0	4
3-Inspect	3	3	0	0	0	0	0	0	3
5-Barcode Server	1	1	0	0	0	0	0	0	1
7-Queue	5	5	0	0	0	0	0	0	5
9-Scan Low	3	3	0	0	0	0	0	0	3

Figure 229: Queue Job Count tab

To view the number of jobs in selected queues, proceed as follows:

1. To display all queues in the application, click **Show Queues**.
2. In the table, select one or more queues.
3. Click **Show Selected Info**.

The number of jobs in the selected queues is displayed.

The last columns display the number of jobs remaining in the queue for less than 1, 2, or 3 hours, or more than 3 hours. For example, the column **3h in queue** shows parcels that were sent to the node more than 2 hours but less than or equal to 3 hours ago.

For information on configuring job hours and column names, see [Viewing User Job Statistics](#).

For more information on the **Queue Job Count** tab, see [Workload Distribution Monitor Queue Job Count Tab](#).

Understanding the Workload Distribution Monitor Window

This section describes the **Workload Distribution Monitor** window. The following topics are included in this section:

- [Workload Distribution Monitor Window Buttons](#)
- [Workload Distribution Monitor Parcels List Tab](#)
- [Workload Distribution Monitor User Job Count Tab](#)
- [Workload Distribution Monitor Queue Job Count Tab](#)

Workload Distribution Monitor Window Buttons

The following tables describe the **Workload Distribution Monitor** window buttons:

Workload Distribution Monitor buttons	
Button	Description
Distribute	Distributes parcels to queues.
Find	Locates parcels within the workflow.
Print	Specifies printing options and prints a report about the selected parcels. For more information on printing reports, see Printing a Report .
Parallel	Displays the parallel parcels of the selected parcel.
Delete Parcel	Deletes the selected parcels and their associated documents. For more information on deleting parcels, see Deleting Parcels .
Reassign User	Reassigns a parcel to another user for processing. For more information on reassigning parcels, see Reassigning a Parcel .
Save Config.	Saves the Workload Distribution Monitor current configuration.
Help	Opens Help.
Close	Closes the Workload Distribution Monitor window.
Delete Doc.	Deletes the selected documents from the queues.
Recover	Restores a locked document. Documents are locked if there is a system interruption during the editing process.
Modify	Opens the selected document in DMS Viewer for editing.
View	Opens the selected document in DMS Viewer for viewing only.
Select All	Selects all parcels in the displayed listing.

Workload Distribution Monitor Parcels List Tab

The following table describes the Workflow Distribution Monitor **Parcels List** tab:

Workflow Distribution Monitor Parcels List tab	
Name	Description
Queue selections	Selects the queue to monitor.
User	Selects the user to monitor.
Calculate Counters	Displays parcel data in the Counters section.
Populate	Displays parcel data in the Counters section and the following table according to specified criteria.

Workflow Distribution Monitor Parcels List tab	
Name	Description
Total	Total number of parcels.
Active	Number of parcels being processed.
Pending	Number of parcels on hold.
Expired	Number of overdue parcels.
Rendezvous	Number of parcels waiting to be reunited with parallel parcels in a specified rendezvous queue.
User	User ID.
Batch #	Batch number.
Parcel #	Parcel number.
Folder #	Folder number.
Pr	Parcel priority as follows: <ul style="list-style-type: none"> • N: Normal • H: High
St	Parcel status as follows: <ul style="list-style-type: none"> • A: Active • H: Hold • E: Expired • R: Rendezvous
Active	Date when parcel is active.
Received on	Date and time parcel was received in current node.
Queue	Parcel's current queue.
Doc ID	Document ID.
Doc Type	Document type.
Created on	Document creation date.
Pages	Number of pages in document.
Queue	Document's current queue.
Locked	Document status. Y indicates that the document is checked out for editing.

Workload Distribution Monitor User Job Count Tab

The following table describes the Workflow Distribution Monitor **User Job Count** tab:

Workflow Distribution Monitor User Job Count tab	
Name	Description
Queue Selections	Selects the queue to monitor.
Show Users	Lists the user IDs of all users with jobs in the selected queue.
Show Selected Info	Displays user information for the selected user IDs.

Workflow Distribution Monitor User Job Count tab	
Name	Description
Configure Hour Columns	Opens the Configure Job Hour Columns window for configuring job hours and column names as described in Viewing User Job Statistics .
User	User ID for which the job count is displayed.
Parcel	Total number of parcels for the user in the selected node.
Active	Number of parcels being processed by the user in the selected node.
Pending	Number of parcels on hold.
Exp	Number of overdue parcels.
Rend	Number of parcels waiting to be reunited with parallel parcels in a specified rendezvous queue.
1 h in queue	Number of jobs in the queue for less than or equal to 1 hour.
2 h in queue	Number of jobs in the queue for more than 1 hour and less than or equal to 2 hours.
3 h in queue	Number of jobs in the queue for more than 2 hours and less than or equal to 3 hours.
> 3 h in queue	Number of jobs in the queue for more than 3 hours.

Workload Distribution Monitor Queue Job Count Tab

The following table describes the Workflow Distribution Monitor **Queue Job Count** tab:

Workflow Distribution Monitor Queue Job Count tab	
Name	Description
Show Queues	Displays queues containing jobs.
Show Selected Info	Displays information about the selected queue.
Configure Hour Columns	Opens the Configure Job Hour Columns window for configuring job hours and column names.
Queue	Queue name.
Parcel	Total number of parcels.
Active	Number of active parcels.
Pending	Number of pending parcels.
Exp	Number of overdue parcels.
Rend	Number of parcels waiting to be reunited with parallel parcels in a specified rendezvous queue.
1 h in queue	Number of jobs in the queue for less than or equal to 1 hour.
2 h in queue	Number of jobs in the queue for more than 1 hour and less than or equal to 2 hours.
3 h in queue	Number of jobs in the queue for more than 2 hours and less than or equal to 3 hours.

Workflow Distribution Monitor Queue Job Count tab	
Name	Description
> 3 h in queue	Number of jobs in the queue for more than 3 hours.

Note: For information on configuring job hours and column names, see [Viewing User Job Statistics](#).

Dealing with Problematic Documents

The **Work Item Notes** window displays jobs that users consider problem jobs. To make the problem job known, users send a note via the Retrieve object to the administrator describing the problem. To see the work item notes, click **Work Item Notes**.



The **Work Item Notes** window appears.

Work Item Notes								
Delete Note		Find Parcel		Save Config.			Close	
Date	User	Station	Doc#	Parcel #	Folder#	Node	Notes	
5/11/2001 12:06:49 PM	DTM	25	2	2	1	3-Queue	Invalid data. Please verify.	
5/11/2001 12:07:18 PM	DTM	25	59	59	999999999	3-Queue	Corrupted data. Re-scan.	

Figure 230: Work Item Notes window

The list of problem notes is shown in a table with the following basic information regarding the note:

- date written
- user name and workstation ID of the sender
- document, parcel, and folder number
- queue where the parcel is located
- note text

To redistribute the problematic document, proceed as follows:

1. Select the record in the table and click **Find Parcel**.

The **Batch/Parcel List** window appears with the selected parcel displayed.

2. Correct the problem as needed.
3. When the problem is solved, to delete the record in the **Work Item Notes** window, select it and click **Delete Note**.

Using Document Versioning

Document versioning is available in Workflow Monitor. **Document versioning** allows Exigen Workflow users to maintain different versions of documents. For more information on document versioning, see [Setting Up Document Versioning](#) and the *Exigen Workflow User's Guide*, Appendix B: Document Versioning.

Chapter 7: Statistical Analysis

This chapter describes the Statistics tool, which monitors user performance and productivity. The following topics are described in this section:

- [Overview](#)
- [Viewing Statistics and Reports](#)

Overview

The Statistics tool calculates and displays statistical information for the following processes:

- High Volume Scan
- Low Volume Scan
- Index
- Inspect
- Queue
- Commit

The results from this application can be viewed in graph form and printed for distribution.

Exigen Workflow generates a list displaying a line item for each day and user. Each line item contains following information:

- user ID
- date
- number of batches or parcels
- documents
- pages
- name of the queue and workflow

The lower portion of the window displays the total as well as the average number of batches, documents and pages processed.

Viewing Statistics and Reports

To open the **Statistics** window, proceed as follows:

1. In Exigen Workflow Explorer, select **Administration Tools > Workflow Tools** and double click the **Statistics** icon:



The **Statistics** window appears.

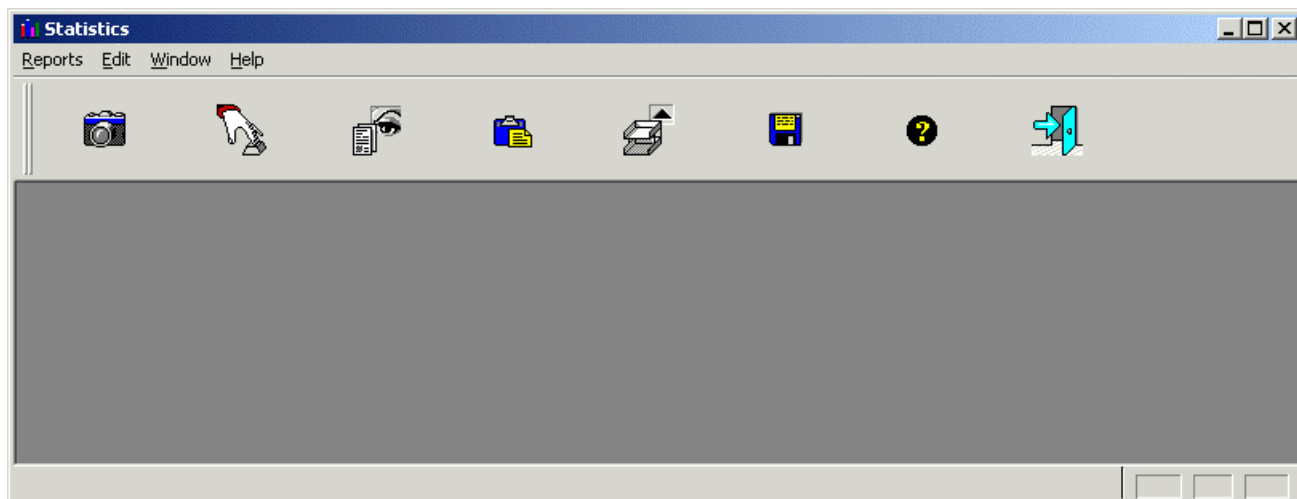







Figure 231: Statistics window

Statistics are displayed based on object class.

2. To view reports for an object class, click the appropriate button listed in the following table:

				
Scan	Index	QA	Miscellaneous	Queues

The corresponding statistics window appears. The window title reflects the object class selected, for example, **Scan Statistics**.

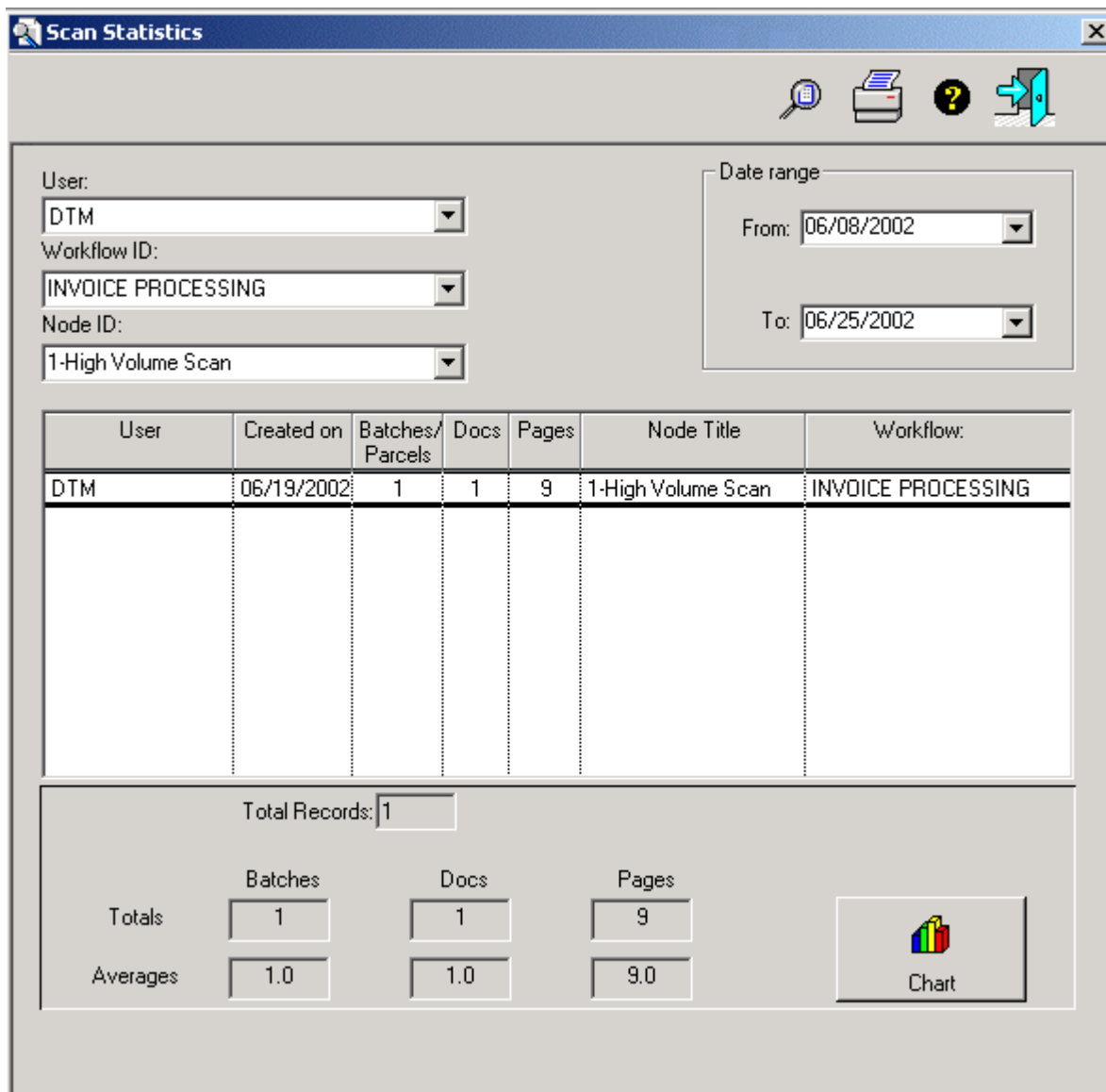


Figure 232: Scan Statistics window

To view the statistics, proceed as follows:

1. In the **Date range** area, select start and end dates.
The default values are for the current day.
2. To specify a user, workflow, and node, select appropriate values in the **User**, **Workflow ID** and **Node ID** lists.
3. To view statistics for all users, workflows, and nodes, leave the corresponding fields blank.
4. To view the statistics, click **Calculate**.



The total numbers of records and averages for the items displayed are shown.

Only one record is displayed for a selected day. For example, if statistics for the current day are retrieved several times, only the latest statistics are displayed.

The **Created on** column displays the time when the user first performed an action in the node on the selected day.

5. To convert the data into a graph format, click **Chart**.

The information is displayed in the **Bar Chart** window.

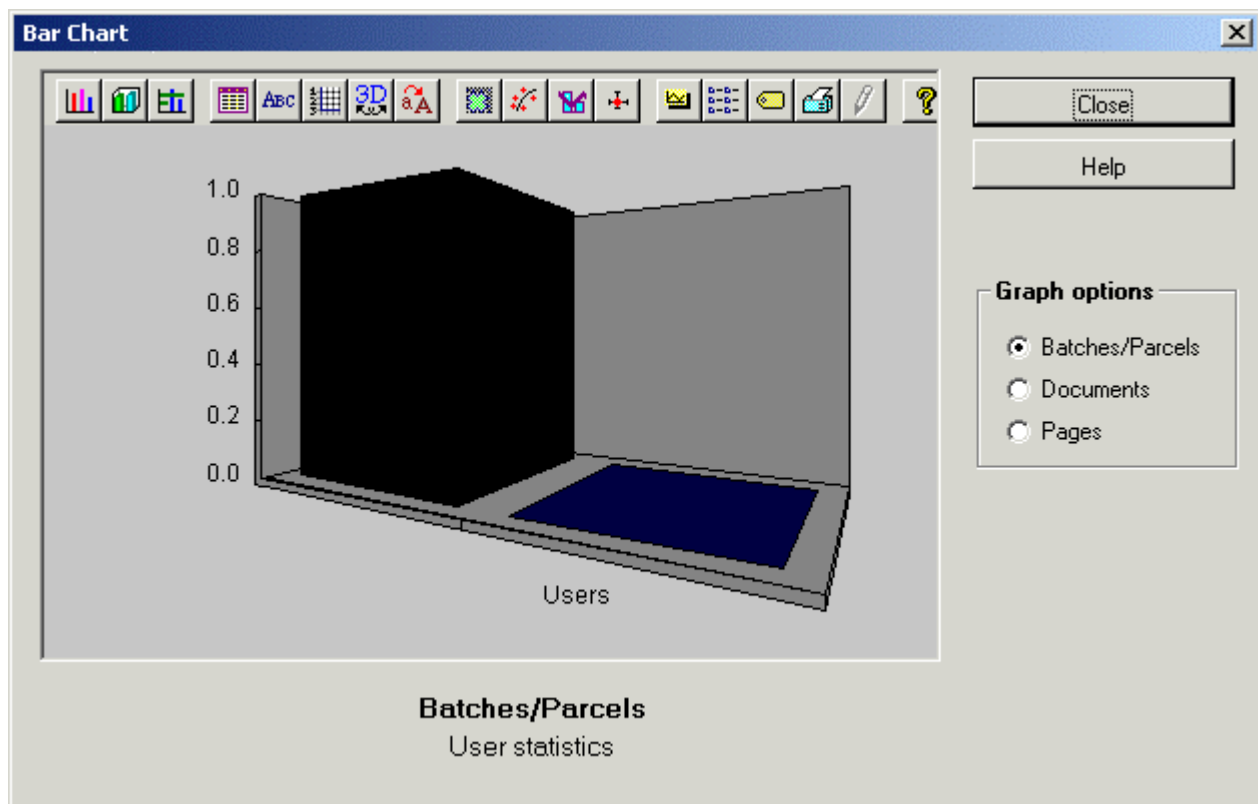


Figure 233: Bar Chart window

6. To print the report, click **Close** and click **Print Report**.



The **Centura Report Builder** window appears with a report file name, for example, `STATS.QRP`.

7. To page through the report, click the browse buttons.
8. To print the report, click **Print**.
9. To close the report, select **File > Close Report** and click **Exit**.



10. To ensure that the **Statistics** window opens to the same size and at the same location the next time it is displayed, click **Save Configuration**.



11. To close the **Statistics** window, click **Exit**.

Note: Statistical records are not produced for Exigen Workflow servers.

Chapter 8: Process Monitor

This chapter explains how to monitor and terminate Exigen Workflow connections. The following topics are described in this section:

- [Overview](#)
- [Using Process Monitor](#)

Overview

The **Process Monitor** application provides a complete picture of all login activity in the entire system. This window allows you to see who is logged into which workflow application and who is using which queue.

Process Monitor also unlocks workstations that improperly or incompletely logged out of a specific queue. A record of the process prohibits the user from logging into the same queue until it is cleared.

Using Process Monitor

To start Process Monitor, in Exigen Workflow Explorer, in the **Workflow Tools** folder, double click the **Process Monitor** icon.



The **Process Monitor** window appears.

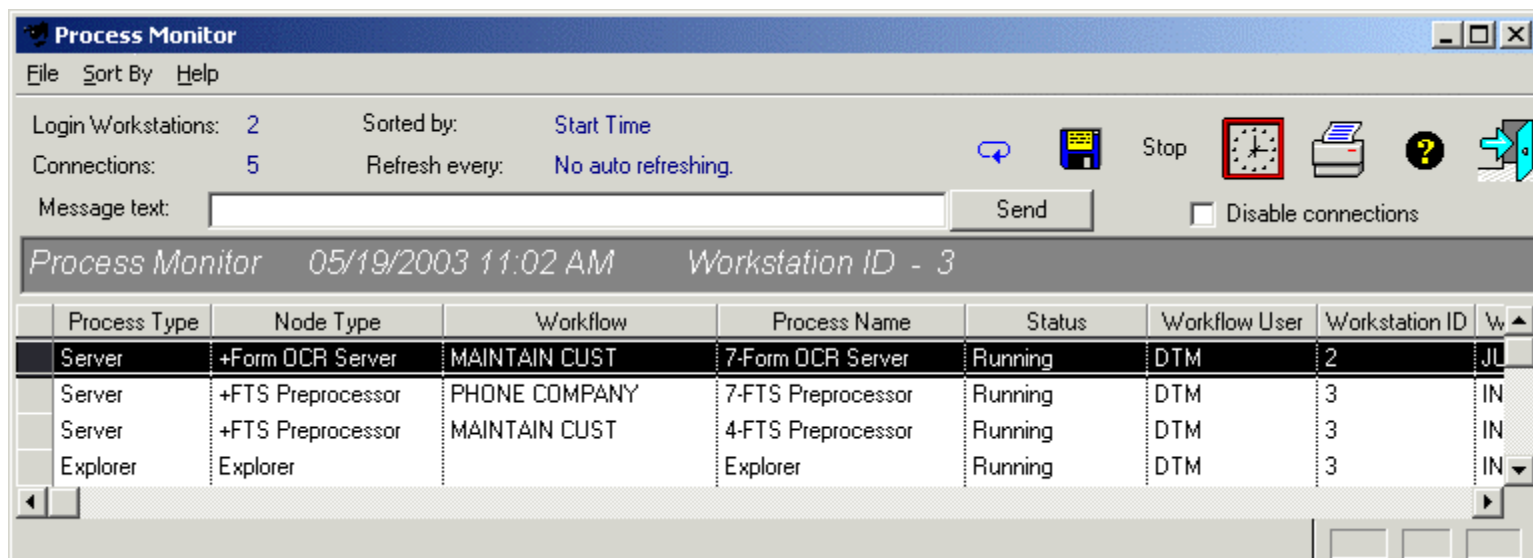


Figure 234: Process Monitor window

The **Process Monitor** window displays the following information:

- number of workstations logged in
- total number of connections
- sort order of the window
- refresh frequency

The following table displays information about the **Process Monitor** window columns:

Process Monitor window columns					
Column	Description				
Process Type	Process type: explorer, object, server/service, database tool, or workflow tool.				
Node Type	Process description if process is launched from a node.				
Workflow	Application name.				
Process Name	Process name.				
Status	Process status: <ul style="list-style-type: none"> • running • not responding • expired • logged out 				
Workflow User	Workflow user.				
Workstation ID	Workstation ID.				
Workstation Name	Workstation name.				
Workstation User	Workstation Windows user.				
Start time	Process starting time.				
Last Update Time	Date and time of last response.				
Requested status	Exit request status: <table border="1"> <tr> <td>Exit</td><td>Request sent to end the selected connection.</td></tr> <tr> <td>Accepted</td><td>User accepted notification on ending the connection.</td></tr> </table>	Exit	Request sent to end the selected connection.	Accepted	User accepted notification on ending the connection.
Exit	Request sent to end the selected connection.				
Accepted	User accepted notification on ending the connection.				

In the **Process Monitor** window, the following tasks are available:

- [Configuring Process Monitor Settings](#)
- [Notifying Users about Stopping a Connection](#)
- [Updating the Connection List](#)
- [Setting the Refresh Frequency](#)
- [Printing the Process Monitor List](#)
- [Sending a Message](#)
- [Disabling Connections](#)
- [Specifying Sort Order](#)
- [Clearing the Process Monitor](#)
- [Saving the Configuration](#)

Configuring Process Monitor Settings

The process monitoring settings configure general process monitoring parameters. To specify process monitor settings, proceed as follows:

1. To access the **Process Monitor Settings** window, in the **Process Monitor** window, select **File > Settings**.

The **Process Monitor Settings** window appears.

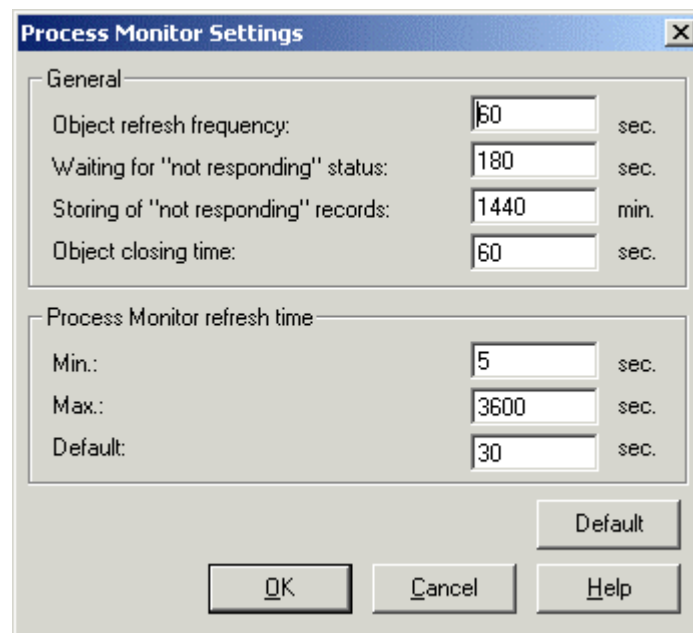


Figure 235: Specifying Process Monitor settings

2. To set how often Exigen Workflow processes report to the system about their current status, in the **Object refresh frequency** field, enter the time.
3. To set the time after which inactive processes in the system are considered to be not responding, in the **Waiting for “Not responding” status** field, enter the time.
4. To set the time for which the not responding process records are kept in the system, in the **Storing of “Not responding” records** field, enter the time.
5. To set the time after which a process is terminated in the system if an administrator stops the process, in the **Object closing time** field, enter the time.
6. To set the minimum Process Monitor refresh time that administrators can enter in the **Set Time for Auto Refreshing** window, in the **Min** field, enter the time.
7. To set the maximum Process Monitor refresh time that administrators can enter in the **Set Time for Auto Refreshing** window, in the **Max** field, enter the time.
8. To set the default Process Monitor refresh time, in the **Default** field, enter the time.
9. To set the default field values for all fields in the **Process Monitor Settings** window, click **Default**.
10. To accept the new parameters, click **OK**.

11. To close the **Process Monitor Settings** window without applying changes, click **Cancel**.

Notifying Users about Stopping a Connection

To end a connection and notify users, select the connection and click **Stop** .

The following occurs:

1. The **Requested status** column displays **Exit**.
2. The connection user receives a message to save any work within a specified time interval.

Note: The time interval is specified in the **Object closing time** field, as described in [Configuring Process Monitor Settings](#).

3. If the user clicks **OK**, the **Requested status** column displays **Accepted**.
4. The connection is stopped after the specified time interval regardless of the user's response.

Updating the Connection List

To update any new or terminated connections in the list, click **Refresh** .

Setting the Refresh Frequency

To set refresh frequency, proceed as follows:

1. Click **Set Timer** .
2. In the **Refresh Process Monitor EverySeconds** field, enter a number.
3. Click **OK**.

Printing the Process Monitor List

To print the Process Monitor list, click **Print** .

Sending a Message

To send a message, proceed as follows:

1. In the table, select a connection.
2. Enter a message text and click **Send**.

Users receive the message within one minute.

Disabling Connections

To disable all connections except Administrator Utility and Process Monitor, select the **Disable connections** check box.

All users who have started their work can continue working, but no new connections are allowed.

Specifying Sort Order

The default sort order for the **Process Monitor** window is by workstation. To change the sort order, proceed as follows:

1. Select the **Sort By** menu.
2. Select one of the following:
 - **Process Type**
 - **Node Type**
 - **Workflow**
 - **Process Name**
 - **Status**
 - **Workflow User**
 - **Workstation ID**
 - **Workstation Name**
 - **Workstation User**
 - **Start Time**
 - **Last Activity Time**
 - **Last Update Time**
 - **Requested status**

You can also sort data by double clicking the column header.

Clearing the Process Monitor

If a record exists in the Process Monitor log and other users attempt to log in to the same queue, they receive the following message:

```
This queue is in use by Workstation XX(<windows workstation name>), user YY
```

For example:

```
This queue is in use by Workstation 12(JENNY), user DTM.
```

To clear Process Monitor and allow another user to log in to the queue, proceed as follows:


1. In the **Process Monitor** window, select the record.
2. Press **F8**.

The record is cleared and the user can proceed into the queue.

Note that any genuinely active processes must not be removed from the list.

Saving the Configuration

To ensure that the **Process Monitor** window opens at the same size and location the next time it is displayed, use any of the following methods:

- Click **Save Configuration** .
- Select **File > Save Configuration**.

Chapter 9: Setting Up Exigen E-Capture

This chapter introduces Exigen E-Capture and describes setup procedures. The following topics are described in this section:

- [Overview](#)
- [Introducing E-Capture Administrator](#)
- [Getting Started](#)
- [Defining Field Types](#)
- [Defining Output Groups](#)
- [Registering Vendors](#)
- [Defining Policy Types](#)
- [Defining Form Categories](#)
- [Registering Special Forms](#)
- [Separating Documents Based on Bookmarks](#)
- [Assigning Diagnoses](#)
- [Registering Companies](#)
- [Using E-Capture Custom Scripts](#)

Overview

Exigen E-Capture is the electronic document management module of Exigen Workflow. E-Capture is used to index and extract data from electronic documents for easy search, retrieval, and handling in Exigen Workflow and other applications.

Exigen E-Capture accepts documents transmitted by corporate network, FTP, and email. It supports the following file types:

File types supported by E-Capture		
Name	Abbreviation	File extension
Portable Document Format	PDF	.pdf
Printer Computer Language	PCL	.pcl

E-Capture supports only PDF versions 1.2-1.5.

Exigen E-Capture consists of the following components:

E-Capture components	
Component	Description
E-Capture Administrator	Configures the E-Capture environment.

E-Capture components	
Component	Description
E-Capture Definition Utility	Registers and maps templates of individual forms so that data can be recognized and extracted.
E-Capture Server	Extracts indexing information from electronic files, converting the files into Exigen Workflow documents, and holding captured information in temporary storage so that it can be used by applications other than Exigen Workflow.

Special Features

The following special features are available in the current version of Exigen E-Capture:

- [Compound Document and Batch Processing Modes](#)
- [Ease of Customization](#)
- [Flexible Data Export](#)

Compound Document and Batch Processing Modes

Exigen E-Capture is run in one of two modes:

- Compound Document Mode
- Batch Processing Mode

In **Compound Document Mode**, a processed file, which may consist of many different forms, is converted into a single Exigen Workflow document.

In **Batch Processing Mode**, a processed file is separated into several Exigen Workflow documents.

Exigen E-Capture automatically separates, indexes, and processes the batch file into separate Exigen Workflow documents. It also detects and removes blank pages if required.

One alternative for separating PDF files into Exigen Workflow documents is to use bookmarks. For information on separating documents based on bookmarks, see [Separating Documents Based on Bookmarks](#).

Ease of Customization

You can customize E-Capture Server using Visual Basic®, Java, Perl or any script language supported by Windows. If you require features not available with Exigen E-Capture's default settings, you can prepare, test, and connect additional scripts to E-Capture Server without changing its basic modules.

Flexible Data Export

Exigen E-Capture can place information into temporary storage to make it available to applications other than Exigen Workflow.

Introducing E-Capture Administrator

Administrator is the administrative module of Exigen E-Capture. You can use Administrator to set up the E-Capture environment.

Important Administrator tasks include the following:

- defining the types of information that you want to index
- registering special forms, form categories, policy types, form software vendors, and in-house divisions and departments
- configuring data export to Exigen Workflow
- registering custom scripts and error handling procedures

Getting Started

To start E-Capture Administrator, proceed as follows:

1. In Exigen Workflow Explorer, select **Administration Tools > Workflow Tools**.
2. Double click the **E-Capture Administrator** icon.



The **Administrator** window appears.

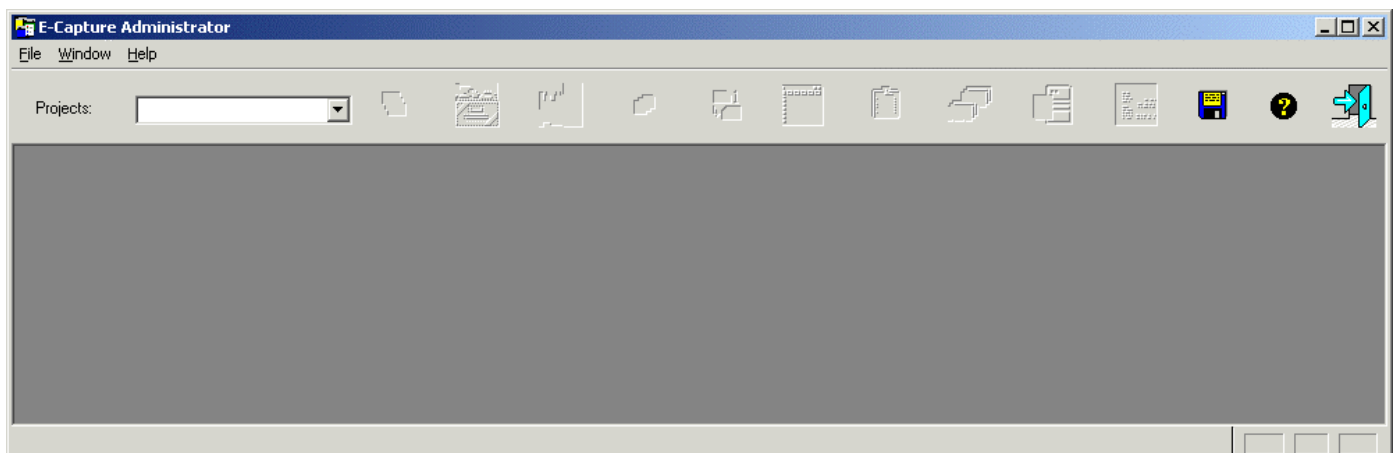


Figure 236: E-Capture Administrator window before selecting a project

Selecting a Project

To enable the **Administrator** toolbar, in the **Project** list box, select an Exigen Workflow project database. All processed documents go to the project you select.

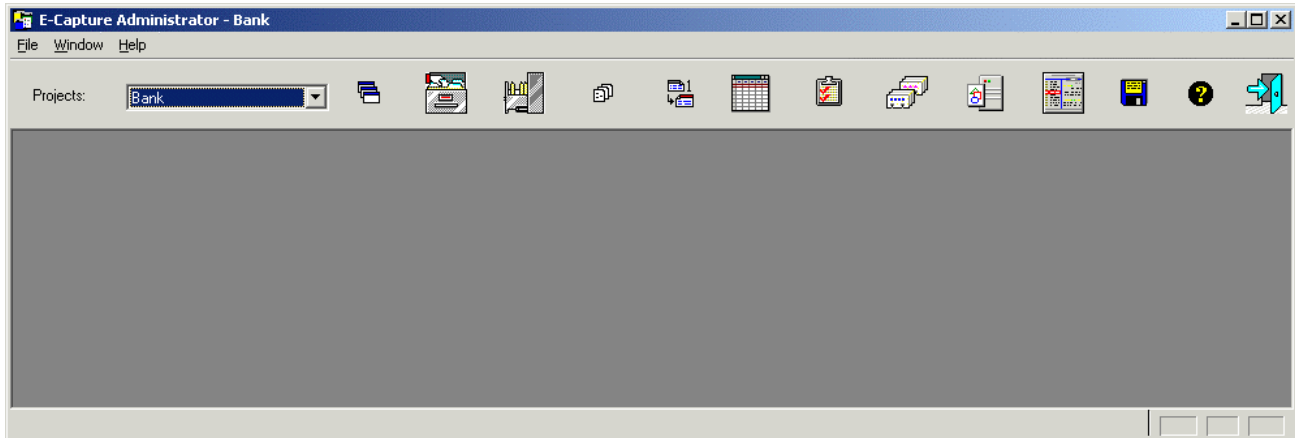




















Figure 237: Selecting a project to enable the Administrator toolbar

The buttons in the **E-Capture Administrator** window are described in the following table:

E-Capture Administrator tools			
Button	Menu option	Shortcut key	Description
	File > Field Types	F2	Defines field types for validating extracted information from documents as described in Defining Field Types .
	File > Output Groups	F3	Defines output groups used to structure information extracted from documents as described in Defining Output Groups .
	File > Vendors	F4	Registers the various software vendors that produce your forms as described in Registering Vendors .
	File > Policy Types	F5	Matches forms to Exigen Workflow Policy Types as described in Defining Policy Types .
	File > Categories	F6	Specifies form sequence in compound documents as described in Defining Form Categories .
	File > Special Forms	F7	Lists forms that require special handling as described in Registering Special Forms .
	File > Diagnoses	F8	Registers error messages to automatically route invalid documents as described in Assigning Diagnoses .

E-Capture Administrator tools			
Button	Menu option	Shortcut key	Description
	File > Companies	F9	Lists the departments and divisions that receive the processed forms as described in Registering Companies .
	File > Registering Modules	F10	Registers modules that require custom scripting as described in Registering Scripted Modules .
	File > Script Maintenance	F11	Assigns and maintains scripts for registered modules as described in Registering Scripts .
	File > Save Configuration		Ensures that the E-Capture Administrator window opens at the same size and location the next time it is displayed.
	Help > Context Help	F1	Opens Help.
	File > Exit	F12	Closes the application.

The windows for the E-Capture tools are similar. Tool buttons are described in the following table:

E-Capture Administrator tool buttons		
Button	Name	Description
	Add	Adds a new element.
	Modify	Modifies the selected element.
	Delete	Deletes the selected element.
	Detail	Shows details of the selected element.
	Exit	Closes the window.

Defining Field Types


Exigen E-Capture field types are used to validate information that Exigen E-Capture extracts from electronic documents.

Examples of field types include number, date/time, currency, and string_4-18. In this last example, E-Capture looks for a string between 4 and 18 characters in length.

You can use field types to validate information such as telephone numbers, email addresses, social security numbers, zip codes, and addresses.

You can specify any criterion as long as you prepare the corresponding script to validate the field. For more information about assigning and maintaining scripts, see [Registering Scripted Modules](#) and [Registering Scripts](#).

At least one field type is mandatory, and is set up by default.

To define field types, in the **Administrator** window, click **Field Types** , to perform the following functions:

- [Adding a Field Type](#)
- [Modifying a Field Type](#)
- [Deleting a Field Type](#)

The **Field Types** window displays all defined field types.

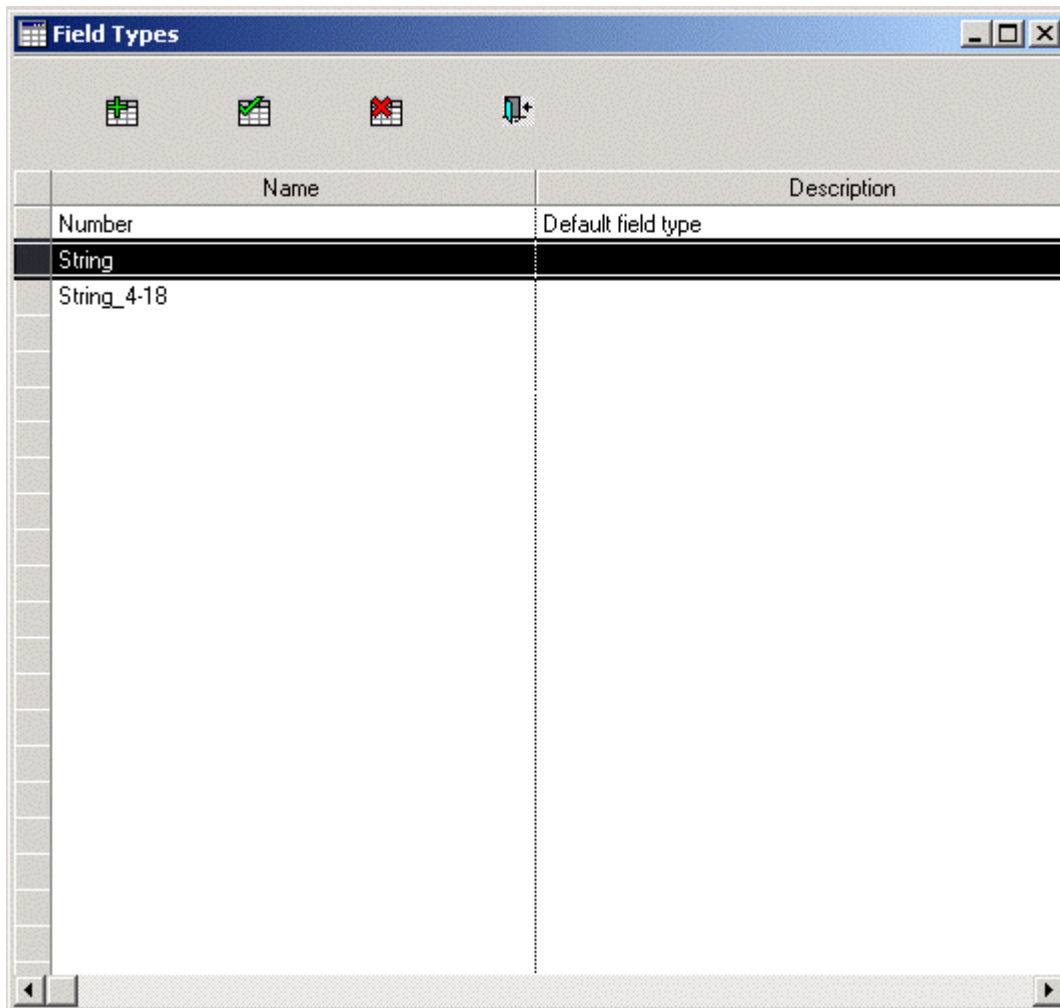


Figure 238: Defining field types

Adding a Field Type

To add a field type, proceed as follows:

1. In the **Field Types** window, click **Add**.



The **Add Field Type** window appears.

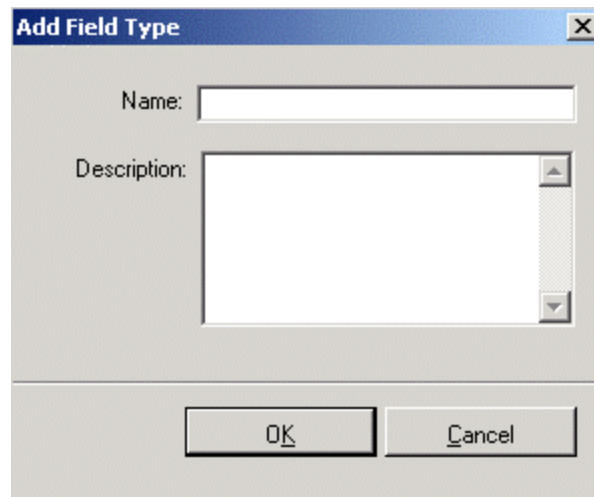


Figure 239: Adding a field type

2. In the **Name** and **Description** fields, enter a field name and description.
3. To save the new field type, click **OK**.

Modifying a Field Type

To modify a field type, proceed as follows:

1. In the **Field Types** window, select a field type.
2. Double click the field type, or click **Modify**.



The **Edit Field Type** window appears.

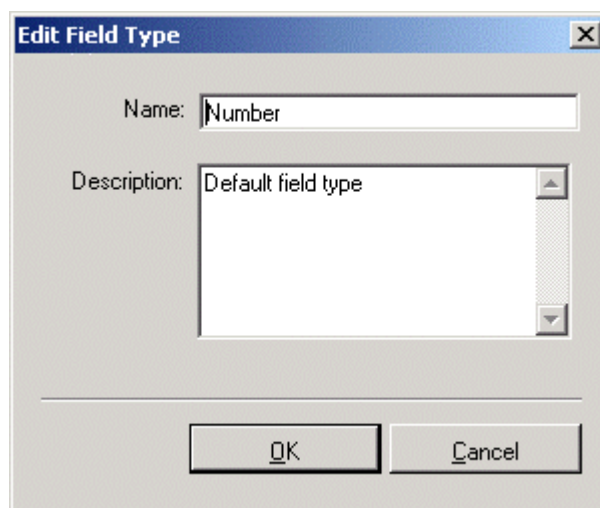


Figure 240: Modifying field type

3. Enter changes to the name and description.
4. To save the changes, click **OK**.

Deleting a Field Type

To delete a field type, proceed as follows:

1. In the **Field Types** window, select a field.
2. Click **Delete**.



A confirmation window appears.

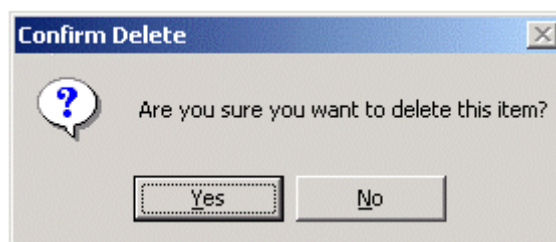


Figure 241: Confirming request to delete field type

3. To delete the field type, click **Yes**.
4. To cancel your request, click **No**.

Note: You cannot delete a field type associated with output details, or a field type that is already assigned to a form in E-Capture Definition Utility. If either condition exists, the error message window appears. For information on output details, see [Defining Output Details](#).

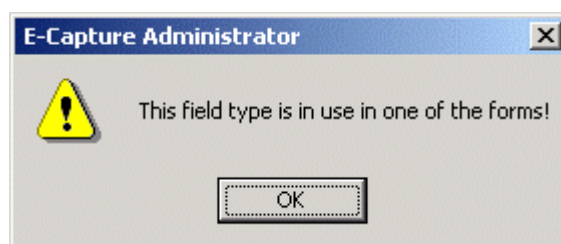


Figure 242: Field type error message

Defining Output Groups

Exigen E-Capture uses output groups to organize information extracted from forms. An output group is a group of fields that contain text you want to capture. Output groups can be assigned to multiple forms.

Each Exigen Workflow project can have many output groups assigned to it, but each output group can only be assigned to one Exigen Workflow project.

Similarly, each output group can have many fields assigned to it, but each output field can only be assigned to one output group.

You must define a minimum of one output group to extract data.

To define output groups, proceed as follows:

1. In the **Administrator** window, click **Output Groups**.



The **Output Groups** window appears and lists the output groups you have already defined. Only the output groups associated with your selected Exigen Workflow project are displayed.

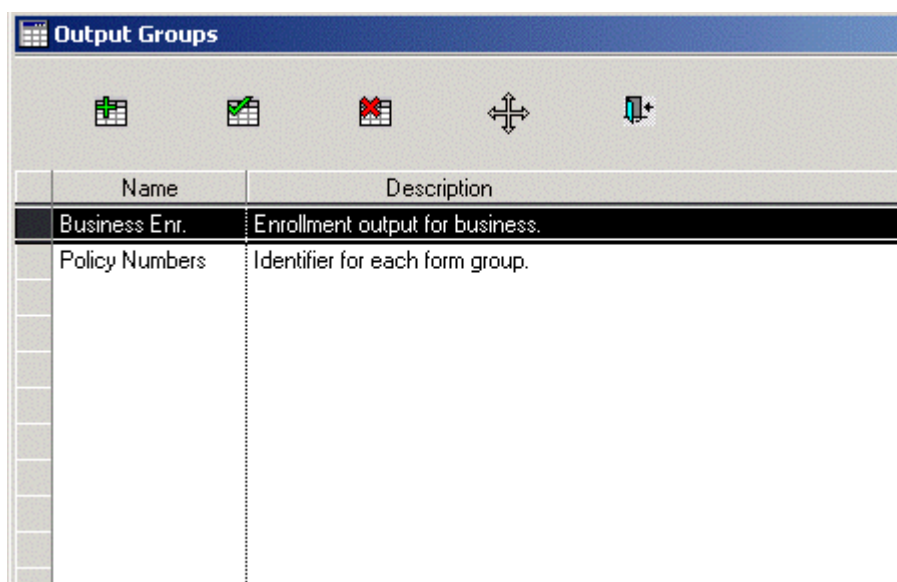


Figure 243: Defining output groups

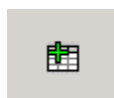
2. Use the **Output Groups** window to perform the following procedures:

- [Adding an Output Group](#)
- [Modifying an Output Group](#)
- [Deleting an Output Group](#)
- [Defining Output Details](#)

Adding an Output Group

To add an output group, proceed as follows:

1. In the **Output Groups** window, click **Add**.



The **Add Output Definition** window appears.

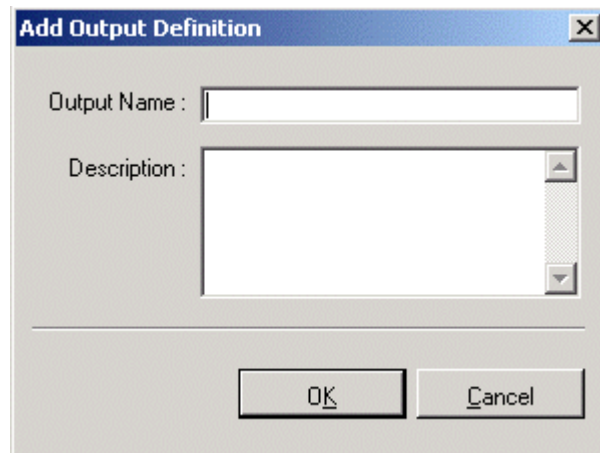


Figure 244: Adding an output group

2. Enter a name and description.
3. To save the new output group, click **OK**.

The output group is automatically assigned to your selected Exigen Workflow project.

Modifying an Output Group

To modify an output group, proceed as follows:

1. In the **Output Groups** window, select the output group to modify.
2. Double click the output group, or click **Modify**.



The **Edit Output Definition** window appears.

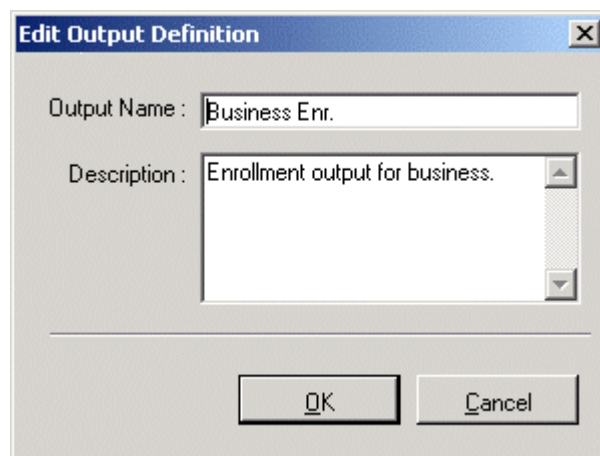


Figure 245: Modifying output group

3. Enter changes to the name and description.
4. To save the changes, click **OK**.

Deleting an Output Group

To delete an output group, proceed as follows:

1. In the **Output Groups** window, select the output group to delete.
2. Click **Delete**.



A confirmation window appears.

3. To delete the output group, click **Yes**.
4. To cancel your request, click **No**.

Note: You cannot delete an output group that has output, or that is already assigned to a form in E-Capture Definition Utility. If either condition exists, the error message window appears. For information on output details, see [Defining Output Details](#).

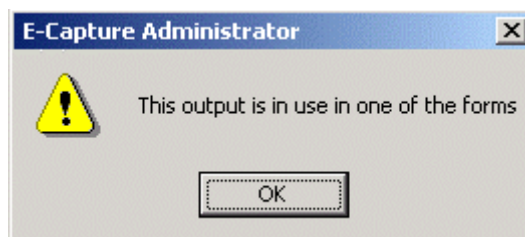


Figure 246: Output group error message

Defining Output Details

An output group comprises any number of output details. These fields label the information you want to capture and assign it to an Exigen Workflow field. Examples of output details are social security number, policy name, and agent identification number.

To define output details, proceed as follows:

1. In the **Output Groups** window, select the output group to which you want to add details.
2. Click **Details**.



The **Output Detail** window displays the name of the selected output group in the title bar.

Field Name	Field Type	Workflow Field	Workflow Field Type	Field Description
Agent	String			
Amount	Number			
e-mail	String	A_EMAIL_ADDR	F	
Policy Number	String	A_MAC_NO	F	
SSN	Number			Refers to policy holders' so

Figure 247: Defining output details

The **Output Detail** window displays the following output details:

- agent
- amount
- email
- policy number
- SSN

The following table describes **Output Detail** attributes:

Output Detail attributes	
Attribute	Description
Field Name	Output detail name. It must be unique.
Field Type	Field type associated with the output detail.
Exigen Workflow Field	Exigen Workflow field name that receives the data.
Exigen Workflow Field Type	Exigen Workflow field type: <ul style="list-style-type: none"> • F: folder • S: subfolder • D: document • B: batchparcel <p>Note: Exigen E-Capture does not support the Document Detail field type.</p>
Field Description	Text description. It is optional.

3. Use the **Output Detail** window to perform the following procedures:

- [Adding an Output Detail](#)
- [Modifying an Output Detail](#)
- [Deleting an Output Detail](#)

Adding an Output Detail

To add an output detail, proceed as follows:

1. In the **Output Detail** window, click **Add**.



The **Add Output Field** window appears.

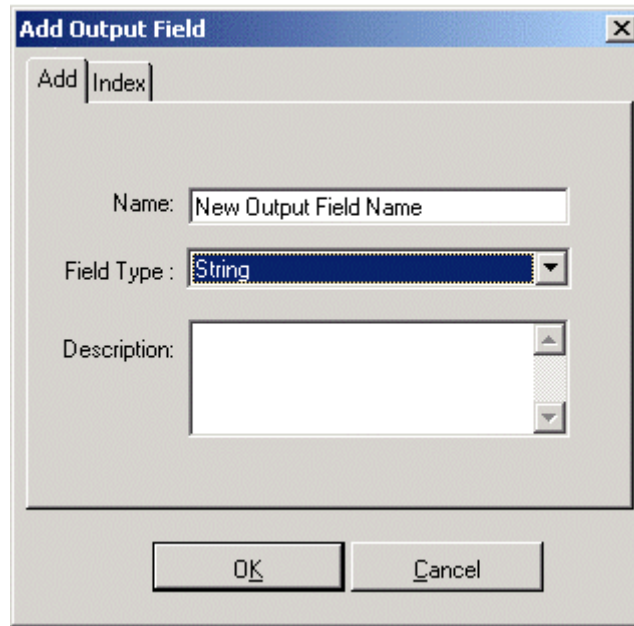


Figure 248: Adding output detail with Add tab

2. In the **Add** tab, enter values in the **Name** and **Description** fields.
3. In the **Field Type** list box, select a field type.
4. To select the destination Exigen Workflow field type and field, in the **Index** tab, select appropriate values in the **Workflow Field Type** and **Workflow Field** lists.

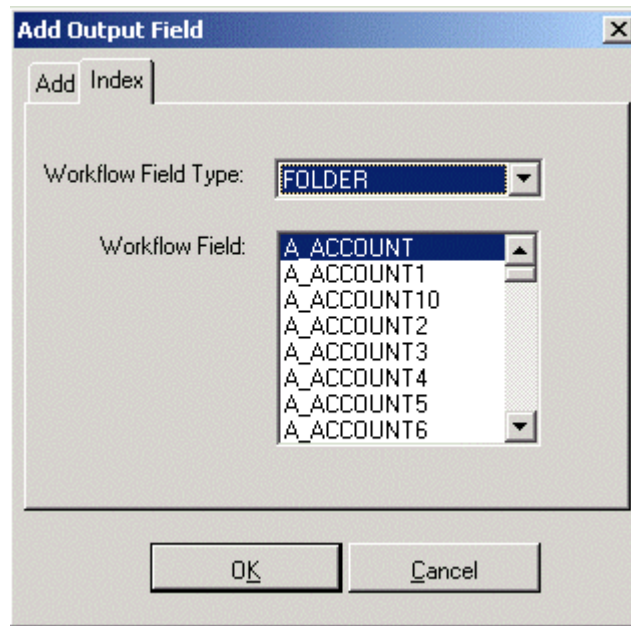


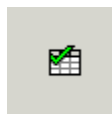
Figure 249: Assigning an Exigen Workflow field and field type

5. To place the information in temporary storage so that it can be used by other applications, in the **Workflow Field Type** list, select **<N/A>**.
6. To save the new output detail, click **OK**.

Modifying an Output Detail

To modify an output detail, proceed as follows:

1. In the **Output Detail** window, select the detail to modify.
2. Double click the detail, or click **Modify**.



The **Edit Output Field** window appears.

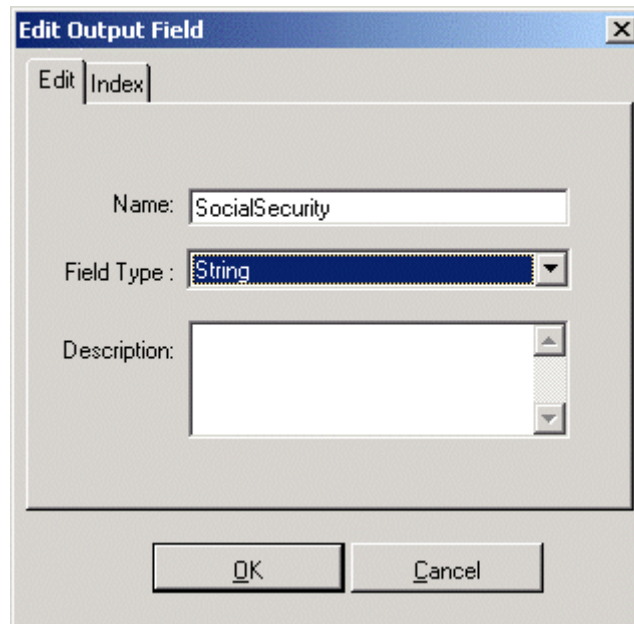


Figure 250: Modifying output detail with Edit tab

3. In the **Edit** tab, in the **Name** and **Description** fields, enter appropriate values.
4. To select a new field type, in the **Field Type** list, select an appropriate value.
5. In the **Index** tab, in the **Workflow Field Type** and **Workflow Field** lists, select appropriate values.

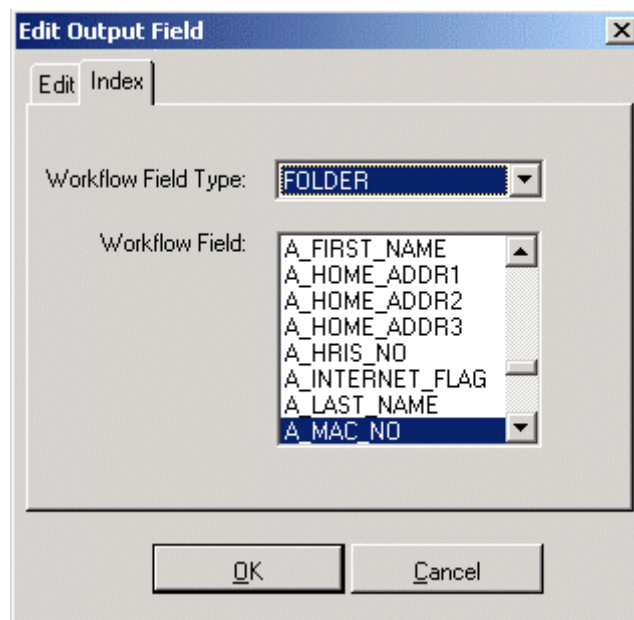


Figure 251: Changing Exigen Workflow field and field type

6. To save changes, click **OK**.

Deleting an Output Detail

To delete an output detail, proceed as follows:

1. In the **Output Detail** window, select the output detail to delete.
2. Click **Delete**.



A confirmation window appears.

3. To delete the output detail, click **Yes**.
4. To cancel the request, click **No**.

Note: You cannot delete an output detail that is already assigned to a form in E-Capture Definition Utility. If this is the case, an error message appears.

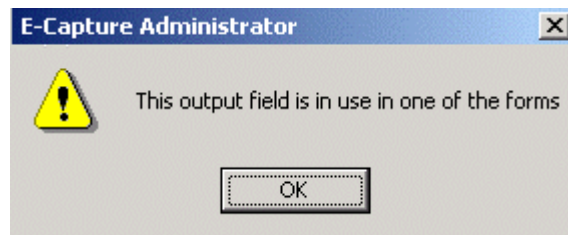



Figure 252: Output field error message

Registering Vendors

E-Capture Administrator provides a software vendor registration interface to accommodate any disparity in text recognition if the same form is created by different software.

To register software vendors, in the E-Capture Administrator window, click **Vendors**  and perform the following procedures:

- [Adding a Software Vendor](#)
- [Modifying a Software Vendor](#)
- [Deleting a Software Vendor](#)

The **Vendors** window displays any registered software vendors.

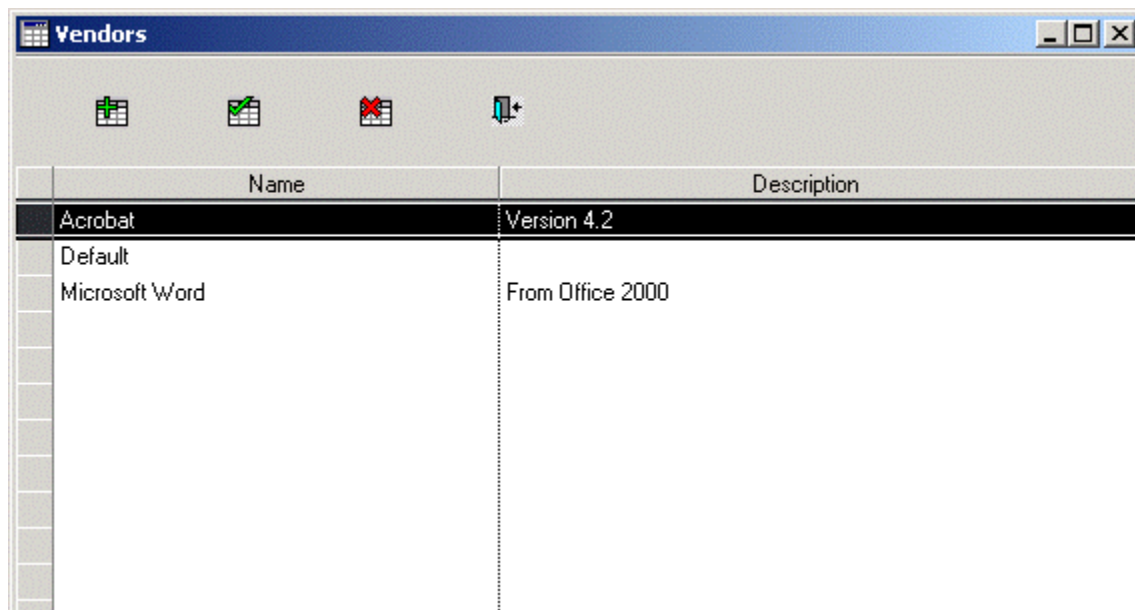


Figure 253: Registering vendors

Adding a Software Vendor

To add a software vendor, proceed as follows:

1. In the **Vendors** window, click **Add**.



The **Add Vendor** window appears.

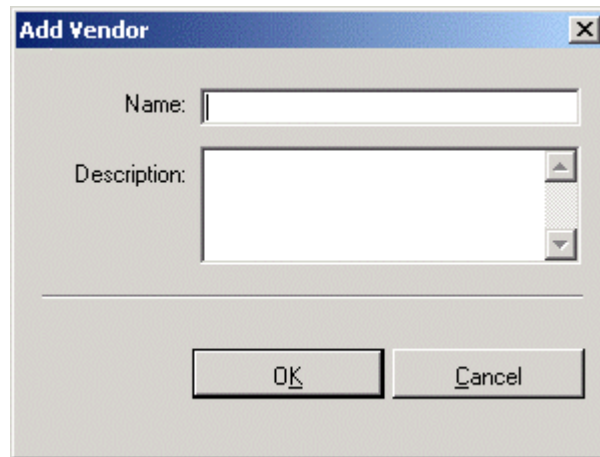


Figure 254: Adding a vendor

2. Enter a software vendor name and description.
3. To save the new vendor, click **OK**.

Modifying a Software Vendor

To modify a software vendor, proceed as follows:

1. In the **Vendors** window, select the vendor to modify.
2. Double click the vendor, or click **Modify**.



The **Edit Vendor** window appears.

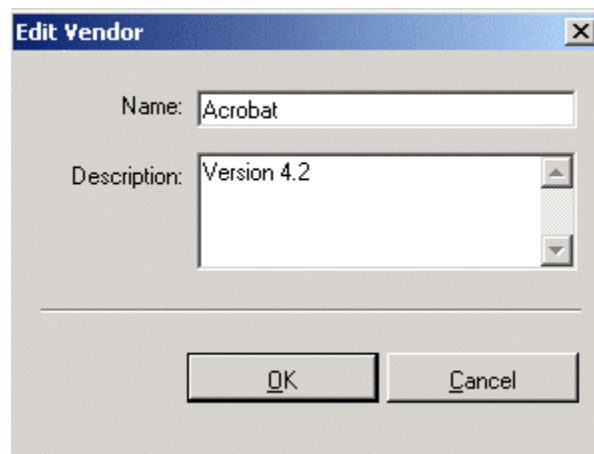


Figure 255: Modifying a vendor

3. In the **Name** and **Description** fields, enter appropriate values.

4. To save changes, click **OK**.

Deleting a Software Vendor

To delete a software vendor, proceed as follows:

1. In the **Vendors** window, select the vendor.
2. Click **Delete**.



A confirmation window appears.

3. To delete the vendor, click **Yes**.
4. To cancel your request, click **No**.

Note: You cannot delete a software vendor that is already assigned to a form in E-Capture Definition Utility. If this is the case, an error message appears.

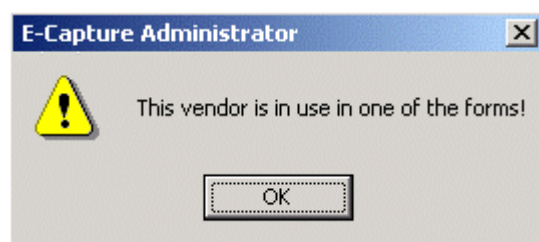


Figure 256: Vendor error message

Defining Policy Types

A policy type is a group of form categories. For example, a policy type named Payments could contain the following form categories:

- Invoices
- Receipts of Payment
- Account Statements

Individual forms are assigned to the relevant form category. Form categories are set up using E-Capture Administrator. For more information on form categories, see [Defining Form Categories](#).

Exigen E-Capture uses policy types to facilitate the sequencing of forms within compound documents. The **Policy Types** tool is used to group categories of forms for processing as described in [Compound Document and Batch Processing Modes](#).

The policy types you define can be the same as your Exigen Workflow document types, but this is not required. The **Default** policy type cannot be deleted.

If you are using batch processing mode, or if you are not concerned with form sequence, skip this step. In this case, documents are assigned to the default policy type. For information on batch processing mode, see [Compound Document and Batch Processing Modes](#).

With custom script, you can customize the way E-Capture recognizes each policy type.

To define policy types, proceed as follows:

1. In the **Administrator** window, click **Policy Types**.



The **Policy Types** window displays all defined policy types.

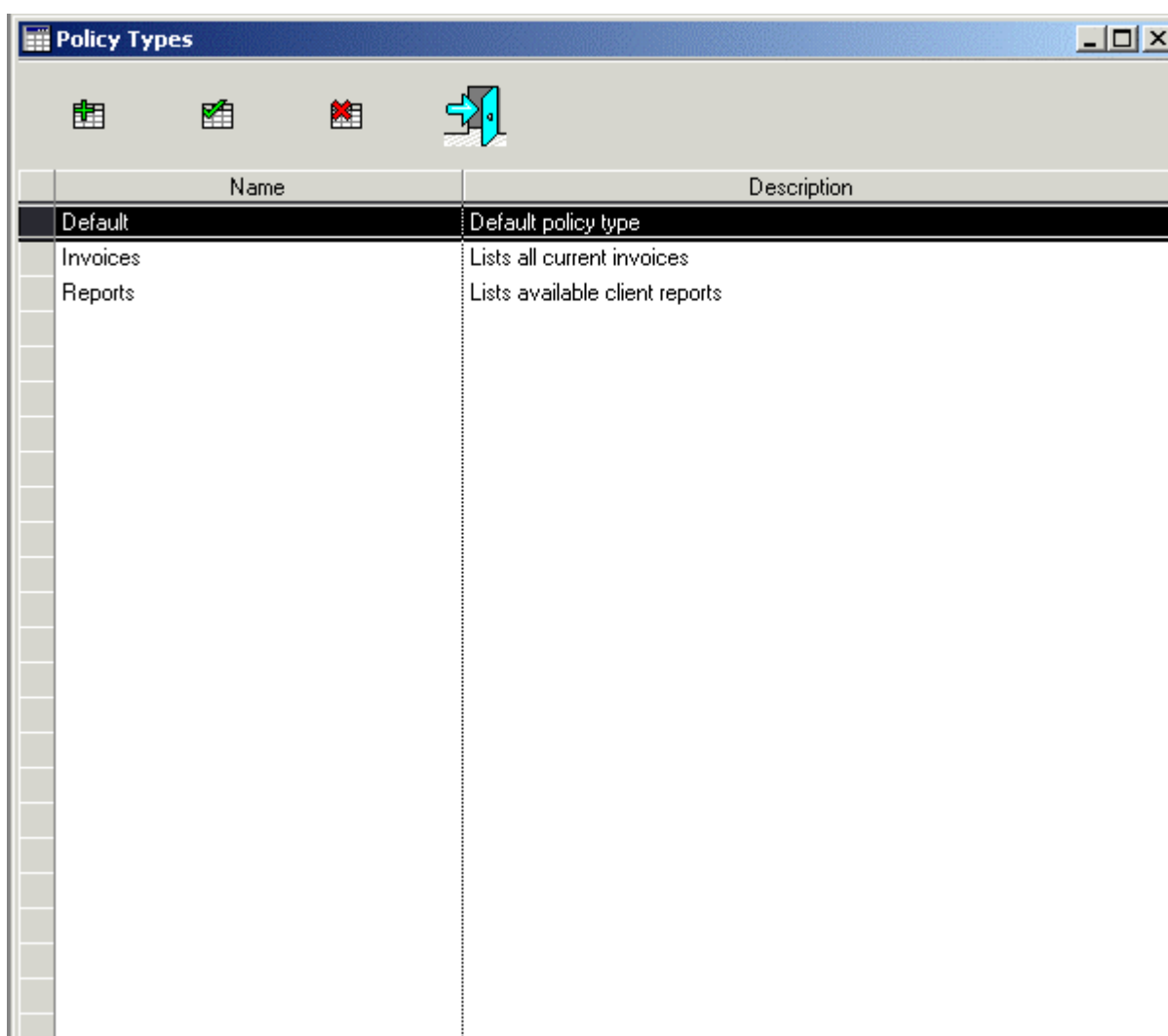


Figure 257: Defining policy types

2. Use the **Policy Types** window to perform the following procedures:
 - [Adding a Policy Type](#)

- [Modifying a Policy Type](#)
- [Deleting a Policy Type](#)

Adding a Policy Type

To add a policy type, proceed as follows:

1. In the **Policy Types** window, click **Add**.



The **Add Policy Type** window appears.

A screenshot of the 'Add Policy Type' dialog box. It has a title bar with the text 'Add Policy Type' and a close button. Inside, there is a 'Name:' label followed by a text input field. Below that is a 'Description:' label followed by a larger text area with a vertical scrollbar. At the bottom, there are two buttons: 'OK' and 'Cancel'.

Figure 258: Adding a policy type

2. In the **Name** and **Description** fields, enter appropriate values.
3. To save the new policy type, click **OK**.

Modifying a Policy Type

To modify a policy type, proceed as follows:

1. In the **Policy Types** window, select the policy type to modify.
2. Double click the policy type, or click **Modify**.



The **Edit Policy Type** window appears.

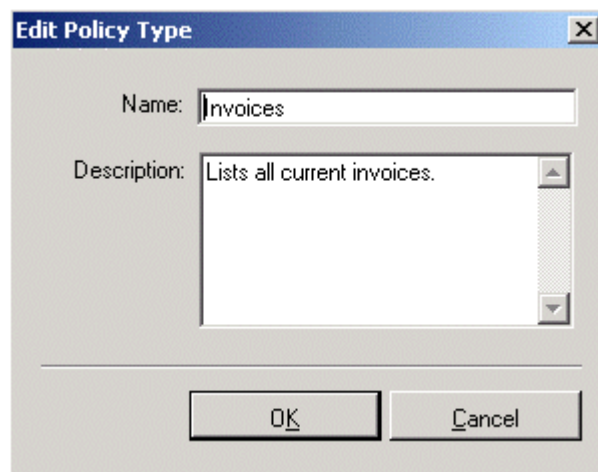


Figure 259: Modifying a policy type

3. In the **Name** and **Description** fields, enter appropriate values.
4. To save your changes, click **OK**.

Deleting a Policy Type

To delete a policy type, proceed as follows:

1. In the **Policy Types** window, select the policy type to delete.
2. Click **Delete**.



A confirmation window appears.

3. To delete the policy type, click **Yes**.
4. To cancel your request, click **No**.

Defining Form Categories

A form category is a logical grouping of forms within a policy type. For example, all form types used for customer evaluation can be grouped into a form category named *Evaluations*.

The **Form Categories** tool is used to sequence forms within the policy types. The sequence you determine is the order in which forms are placed in an Exigen Workflow document.

A form category is not assigned exclusively to one policy type. Each form category is available to all policy types.

All forms not assigned to another category are assigned to the **Default** category. You can place the **Default** category in any order.

To define form categories, proceed as follows:

1. In the **Administrator** window, click **Form Categories**.



The **Form Categories** window displays all defined categories.

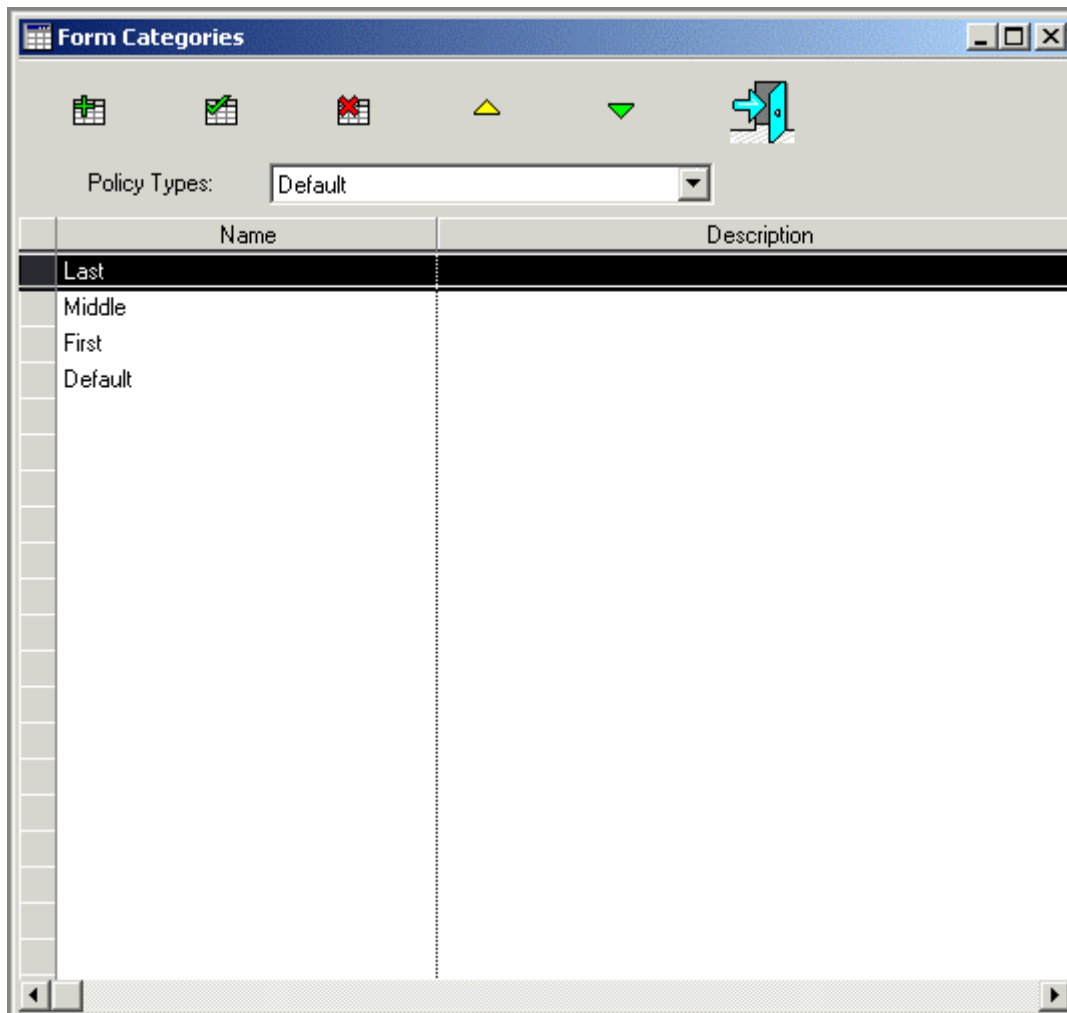


Figure 260: Defining form categories

The form categories for the selected policy type appear in the order in which you want the forms to be exported to an Exigen Workflow document.

2. To view the sequence of categories of a policy type, in the **Policy Types** list box, select a policy type.
3. Use the **Form Categories** window to perform the following procedures:
 - [Sequencing Form Categories](#)
 - [Adding a Form Category](#)
 - [Modifying a Form Category](#)
 - [Deleting a Form Category](#)

Sequencing Form Categories

To sequence form categories, proceed as follows:

1. In the **Form Categories** window, in the **Policy Types** list box, select the policy type to be sequenced.
2. Select the form category to move.
3. To sequence the categories, click the **Up** and **Down** arrows on the toolbar.

Adding a Form Category

To add a form category, proceed as follows:

1. In the **Form Categories** window, in the **Policy Type** list box, select a policy type.
2. Click **Add**.



The **Add Category** window appears.

The 'Add Category' dialog box is shown. It has a title bar with 'Add Category' and a close button. Inside, there are three fields: 'Name:' with an empty text box, 'Policy Type:' with a dropdown menu showing 'Invoices', and 'Description:' with a large empty text area. Below these fields is a section titled 'Insert into Row' containing three radio buttons: 'First' (selected), 'Last', and 'Above Selected'. To the right of these radio buttons are two arrow buttons (up and down). At the bottom are 'OK' and 'Cancel' buttons.

Figure 261: Adding a form category

The selected policy type appears in the **Policy Types** field.

3. In the **Name** and **Description** fields, enter appropriate values.

- To position the new category in the list, in the **Insert into Row** area, select an option or click the up and down arrows to sequence the categories:

Insert into Row options	
Name	Description
First	Assigns first position.
Last	Assigns last position.
Above Selected	Places the new category above the selected category.

- To save the new category, click **OK**.

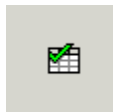
If more than one policy type is registered, the next policy type name appears in the **Policy Type** field.

- Repeat steps 3 through 5 to process all policy types.

Modifying a Form Category

To modify a form category, proceed as follows:

- In the **Form Categories** window, select a policy type.
- Select the form category to modify.
- Double click the category, or click **Modify**.



The **Edit Category** window appears.

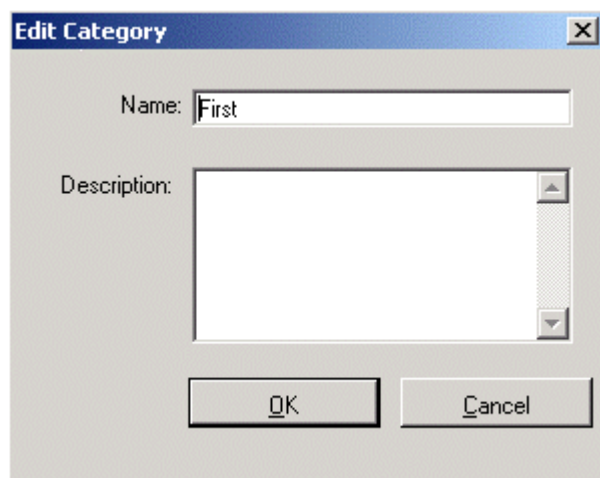


Figure 262: Modifying a form category

- Change the name and description.
- To save the changes, click **OK**.

Deleting a Form Category

To delete a form category, proceed as follows:

1. In the **Form Categories** window, select the form category to delete.
2. Click **Delete**.



A confirmation window appears.

3. To delete the form category, click **Yes**.
4. To cancel your request, click **No**.

Note: You cannot delete a form category that is already associated with a form in E-Capture Definition Utility. If this is the case, an error message appears.



Figure 263: Category error message

Registering Special Forms

The **Special Forms** tool is used to register forms that are used for goals other than routine data extraction. For example, a Schedule of Forms lists all forms contained with a file, and can be used to verify that the file is complete.

Some of the special forms use predefined processing procedures. Other special forms are processed according to rules you define with custom scripts.

You may not require each special form. You can select available forms according to the specific needs of your business.

All supported special forms are predefined. E-Capture currently supports the special forms listed in the following table:

Special forms	
Form type	Description
Regular	Default form type. Most forms are classified as Regular.
Trigger Form	Initiates a corresponding script to achieve desired trigger actions.

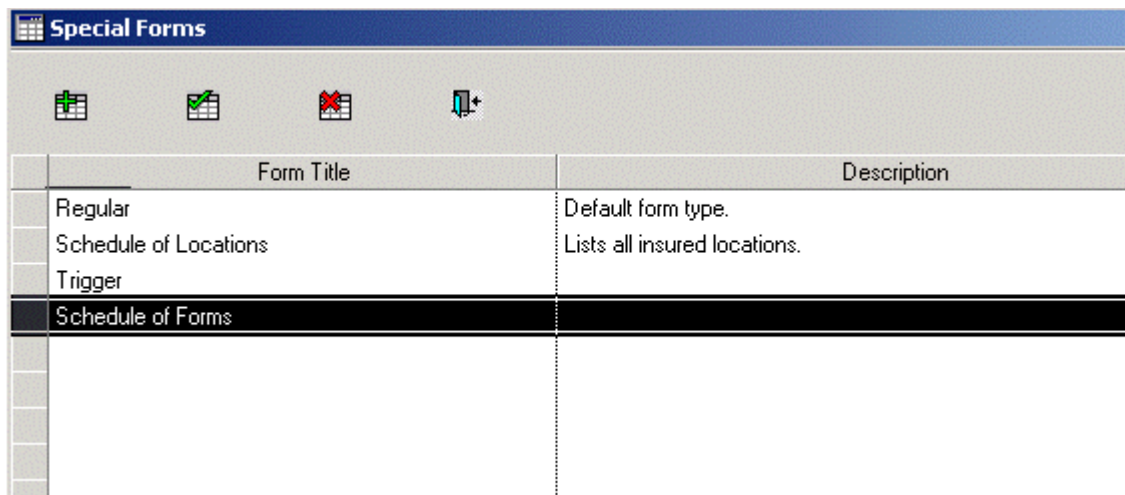
Special forms	
Form type	Description
Separator	First page of each form inside a batch file. These forms are exported to Exigen Workflow as separate documents. In Batch Processing Mode, you must register a separator. For more information on Batch Processing Mode, see Compound Document and Batch Processing Modes .
Schedule of Forms	Lists the most important forms in a compound document. Information is extracted according to default settings.
Schedule of Locations	Standard insurance industry form from which information is extracted according to default settings.
Schedule of Named Insured	Standard insurance industry form from which information is extracted according to default settings.
MASTER	<p>Form for separating PDF files into Exigen Workflow documents and extracting information.</p> <p>The MASTER template specifies the information that must be extracted and the location of the information.</p> <p>Multiple MASTER templates can be applied to a single PDF file that consists of many documents.</p>
SLAVE	<p>Form for separating PDF files into Exigen Workflow documents without extracting indexing or other information from the content of the recognized document.</p> <p>SLAVE documents derive indexing and other information from the last document recognized by the MASTER form.</p> <p>Each SLAVE document is automatically associated with the preceding MASTER document. If a SLAVE document has no associated MASTER document, the SLAVE document is assigned to the default folder.</p> <p>Several SLAVE documents can use folder and subfolder information from a single MASTER document.</p>

To register special forms, proceed as follows:

1. In the **Administrator** window, click **Special Forms**.



The **Special Forms** window displays any registered form types.

The image shows a window titled "Special Forms" with a toolbar containing four icons: a green plus sign, a green checkmark, a red X, and a blue plus sign. Below the toolbar is a table with two columns: "Form Title" and "Description".

Form Title	Description
Regular	Default form type.
Schedule of Locations	Lists all insured locations.
Trigger	
Schedule of Forms	

Figure 264: Registering special forms

2. Use the **Special Forms** window to perform the following procedures:

- [Adding a Special Form](#)
- [Modifying a Special Form](#)
- [Deleting a Special Form](#)

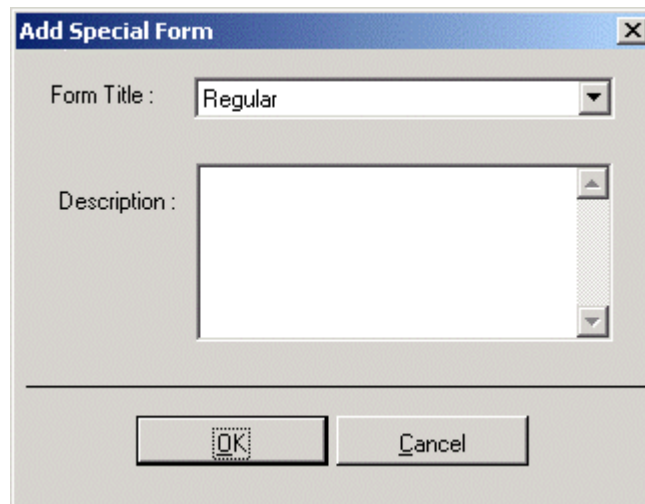
Adding a Special Form

To add a special form, proceed as follows:

1. In the **Special Forms** window, click **Add**.



The **Add Special Form** window appears.

The image shows a dialog box titled "Add Special Form" with a close button (X) in the top right corner. It contains two fields: "Form Title" with a dropdown menu showing "Regular", and "Description" with a large text area. At the bottom are "OK" and "Cancel" buttons.

Form Title : Regular

Description :

OK Cancel

Figure 265: Adding a special form

2. In the **Form Title** list, select a special form.
3. In the **Description** field, enter a form description.
4. To save the new form, click **OK**.

Modifying a Special Form

To modify a special form, proceed as follows:

1. In the **Special Forms** window, select a form.
2. Double click the form, or click **Modify**.



The **Edit Special Form** window appears.

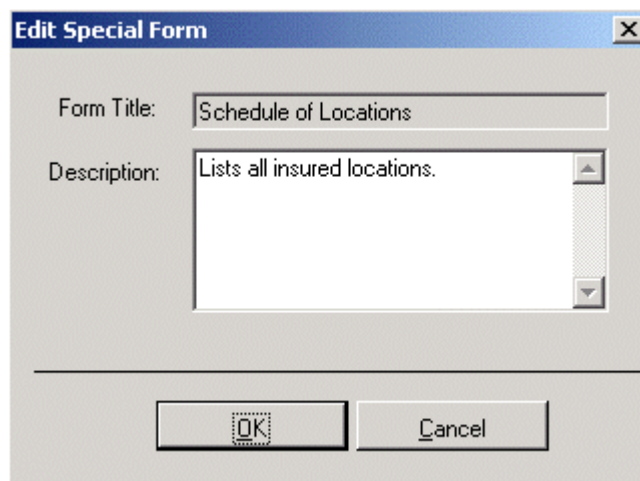


Figure 266: Modifying a special form

3. In the **Description** field, enter appropriate values.
4. To save the changes, click **OK**.

Deleting a Special Form

To delete a special form, proceed as follows:

1. In the **Special Form** window, select a form.
2. Click **Delete**.



A confirmation window appears.

3. To delete the special form, click **Yes**.
4. To cancel your request, click **No**.

Note: You cannot delete a special form that is already associated with a form in E-Capture Definition Utility. If this is the case, an error message appears.

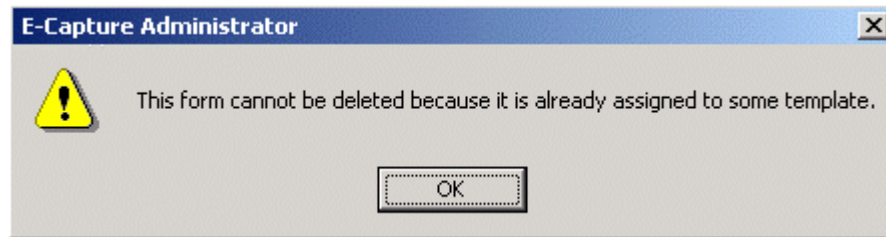


Figure 267: Error message when deleting a form

Separating Documents Based on Bookmarks

The following topics are described in this section:

- [Overview](#)
- [Restrictions](#)
- [Setting Up the Separation of PDF Files Based on Bookmarks](#)

Overview

Automatically produced PDF files that are composed of multiple documents can contain bookmarks pointing to the documents. If E-Capture is set up to automatically separate PDF files into Exigen Workflow documents based on bookmarks, the time usually required for registering and mapping multiple templates is reduced. E-Capture Server performance is improved because the server is not required to convert the PDF files into text files or recognize their templates.

When E-Capture splits bookmarked PDF files into Exigen Workflow documents, the indexing information for the documents is extracted from the first document in the file. This document requires a mapped template.

If additional information is required for indexing extracted documents, that information is usually contained in the corresponding bookmark tree. For each processed PDF file, E-Capture can be set up to create a text file containing the information from the bookmark tree. The text file contains all required information for modifying the indexes and document types of existing documents. The best tool for modifying the indexes of existing documents is an Automatic Queue Server script. For more information on Automatic Queue Server scripts, see the *Exigen Workflow Administrator's Guide, Part 2: Business Component Reference*, Chapter 19: Automatic Queue Server, Automatic Queue Server Scripts.

The following figure is a sample text file that is created when a PDF file is processed on the basis of bookmarks:

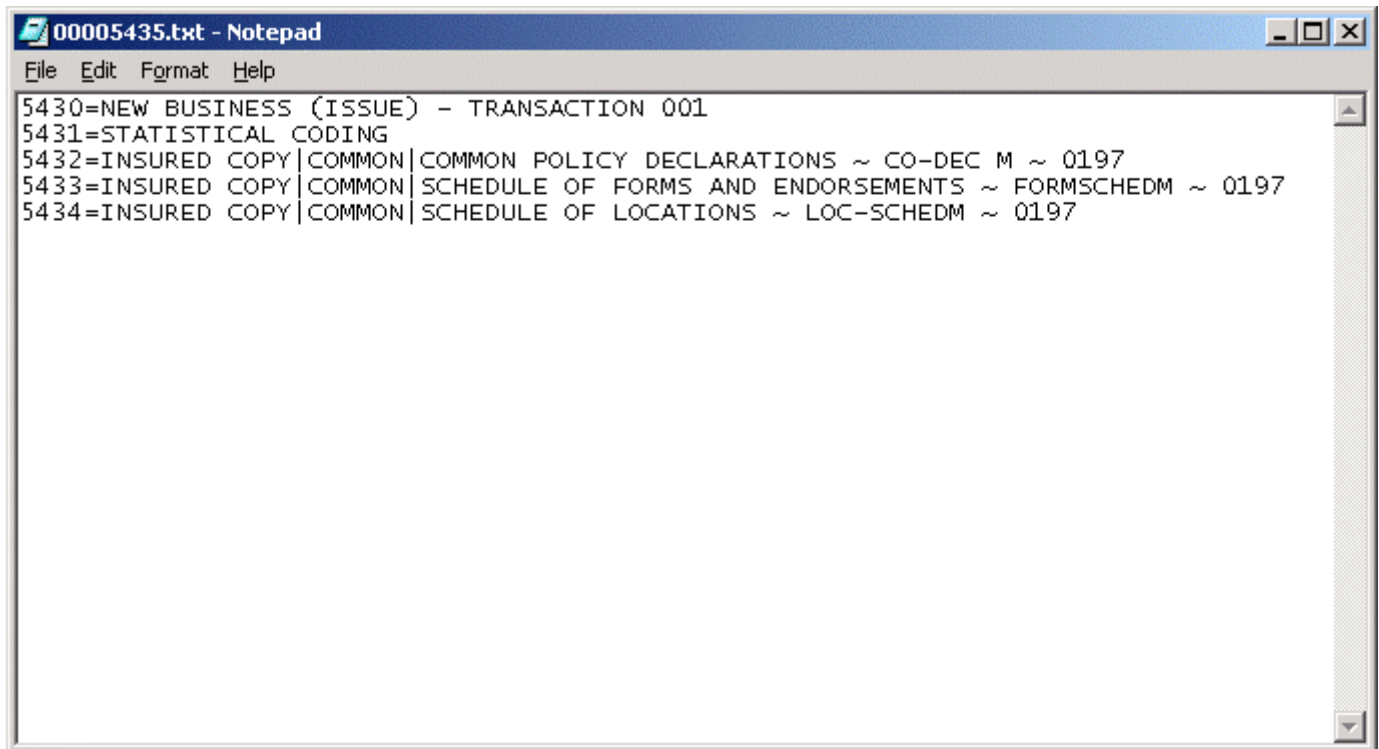


Figure 268: Text document containing additional information

The numbers on the left are Exigen Workflow document numbers.

Each Exigen Workflow document number is associated with a bookmark. Levels in the bookmark tree are delimited by vertical bars.

Restrictions

The following restrictions apply when processing bookmarked PDF files:

- All folder and subfolder information is extracted from the first page of the processed PDF file. A template must be assigned to the first page of the PDF file. Any PDF file that does not have a template assigned to the first page goes to the exception queue.
- In the PDF file, each document must be associated with a bookmark.
- In the PDF file, vertical bars must not appear in bookmark names.
- In the PDF file, each page must be associated with a document.
- In the PDF file, if documents contain multiple pages, one of the following statements must be true:
 - Individual pages do not have bookmarks.
 - Individual pages have bookmarks that always begin with the same word, for example, *Page*. The word is configurable and must be the same for each PDF file going through the same input directory.

Setting Up the Separation of PDF Files Based on Bookmarks

To set up the separation of PDF files into Exigen Workflow documents based on bookmarks, proceed as follows:

1. Review the PDF files to be processed and ensure that all restrictions are observed.

For information on restrictions, see [Restrictions](#).

2. To enable separation based on bookmarks, when setting up E-Capture Server, in the **E-Capture Server Setup: Step 5** window, ensure that the **Use Bookmarks** option is selected.

For information on the **E-Capture Server Setup: Step 5** window, see the *Exigen Workflow Administrator's Guide, Part 2: Business Component Reference*, Adding a Directory Configuration.

3. To ensure that E-Capture Server does not create new folders when processing PDF files, in the **E-Capture Server Setup: Step 5** window, select the **New Folder Is Not Allowed** option.
4. To ensure that the document type of the Exigen Workflow text document created during bookmark separation is displayed, in the **E-Capture Server Setup: Step 5** window, ensure that the **Bookmark Doc Type** option is selected.
5. If the PDF files to be processed contain documents with multiple pages, to assign a rejection keyword to filter out bookmarks that point to individual pages in a multiple page document, in the **E-Capture Server Setup: Step 5** window, in the **Rejection Keyword** field, enter an appropriate keyword.
6. If a rejection keyword is specified, ensure that the keyword is used in the bookmarks of all pages in multiple page documents.

Assigning Diagnoses

Exigen E-Capture provides E-Capture Diagnoses as a convenient solution for delivering information about invalid documents, forms, or data. **E-Capture Diagnoses** are a special set of error codes that address typical business processing problems. The diagnoses can be used, for example, to properly automatically route documents that are missing required information.

The **Diagnoses** tool is used to assign one of the supported diagnoses codes to an Exigen Workflow field. If a problem occurs, the assigned field displays the relevant error code.

More than one diagnosis can be assigned to the same Exigen Workflow field. In this case, the first to be assigned is overwritten by the next.

You may not require each diagnosis. You can select a diagnosis from the available diagnoses according to your specific business requirements.

For more information on diagnoses, see [Appendix E: Diagnoses](#).

To assign diagnoses, proceed as follows:

1. In the **Administrator** window, click **Diagnoses**.



The **Diagnoses** window appears.

Diagnoses				
Problem Code	Workflow Field Type	Workflow Field	Move to Exception Queue	
EMPTY_MANDATORYFIELD	F	A_MAC1	Yes	
EMPTY_TEXT_FILE	F	A_F1	Yes	
FORM_COMPLETENESS	F	A_MAC2	Yes	
IDENTIFIER_NUMBER	F	A_F2	Yes	
NO_FORM_SCHEDULE	F	A_AU	Yes	
NO_FORMS_IN_FILE	F	A_EIN	Yes	
NO_REC_IN_REF_TABLE	F	A_F3	Yes	
NOT_VALID_FIELD	F	A_MAC_NO	Yes	
PAGES_IN_FILE	F	A_COID2	Yes	
SOURCE_FILE_NAME	F	A_COID3	No	
VENDOR_ISSUE	F	A_COID1	Yes	
WRONG_CALCULATIONS	B	A_EIS_ROUTE	Yes	

Figure 269: Assigning diagnoses

The preceding example displays a list of currently supported diagnosis codes, the Exigen Workflow field and field type to which each is assigned, and the status of moving the document to the exception queue.

2. Use the **Diagnoses** window to perform the following procedures:

- [Adding a Diagnosis](#)
- [Modifying a Diagnosis](#)
- [Deleting a Diagnosis](#)

Adding a Diagnosis

To add a diagnosis, proceed as follows:

1. In the **Diagnoses** window, click **Add**.



The **Add New Diagnosis** window appears.

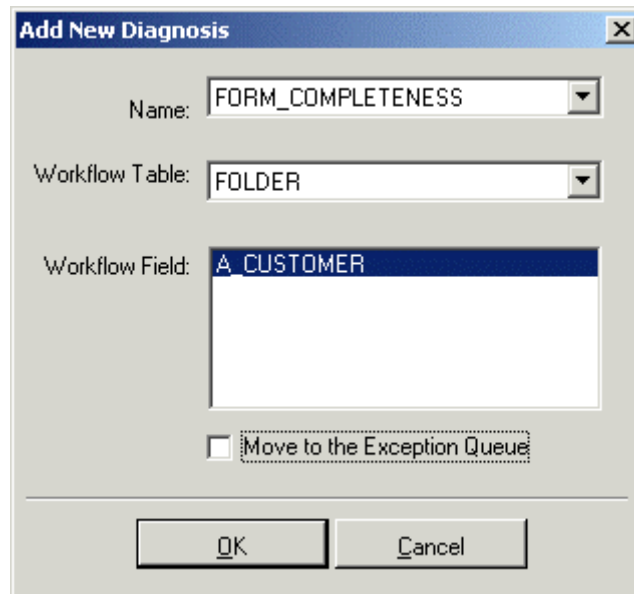


Figure 270: Adding a diagnosis

2. In the **Name** list box, select the diagnosis you want to assign.
3. In the **Workflow Table** list box, select the appropriate Exigen Workflow table type.
4. In the **Workflow Field** list box, select the destination Exigen Workflow field.
5. To move the document to the exception queue, select the **Move to the Exception Queue** checkbox.
6. To save the new assignment, click **OK**.

Modifying a Diagnosis

To modify a diagnosis, proceed as follows:

1. In the **Diagnoses** window, select a diagnosis.
2. Double click the diagnosis, or click **Modify**.



The **Edit Diagnosis** window appears.

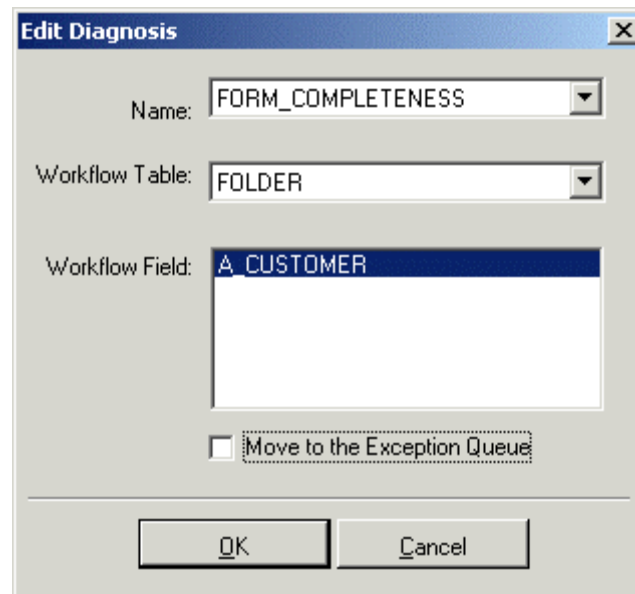


Figure 271: Modifying a diagnosis

3. Update the list boxes as required.
4. To move the document to the exception queue, select the **Move to the Exception Queue** checkbox.
5. To save the changes, click **OK**.

Deleting a Diagnosis

To delete a diagnosis, proceed as follows:

1. In the **Diagnoses** window, select a diagnosis.
2. Click **Delete**.



A confirmation window appears.

3. To delete the diagnosis, click **Yes**.
4. To cancel your request, click **No**.

Registering Companies

The **Companies** tool is used to register internal divisions and departments to which received and processed documents are assigned. This information is required to direct data to Exigen Workflow during transfers and to communicate with other databases.

To register companies, proceed as follows:

1. In the **Administrator** window, click **Companies**.



The **Companies** window displays any registered companies.

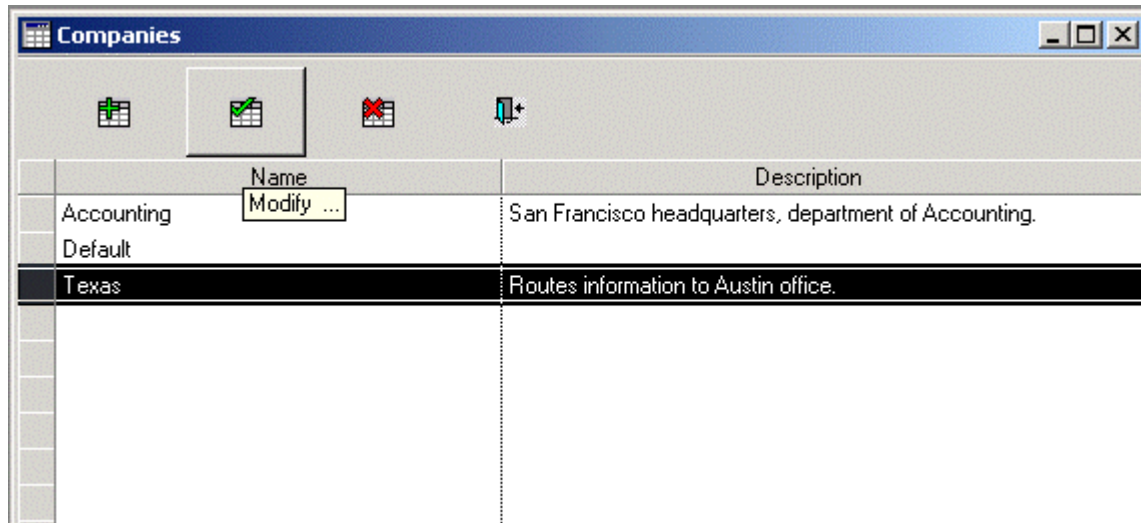


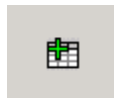
Figure 272: Registering companies

2. Use the **Companies** window to perform the following procedures:
 - [Adding a Company](#)
 - [Modifying a Company](#)
 - [Deleting a Company](#)

Adding a Company

To add a new company, proceed as follows:

1. In the **Companies** window, click **Add**.



The **Add Company** window appears.

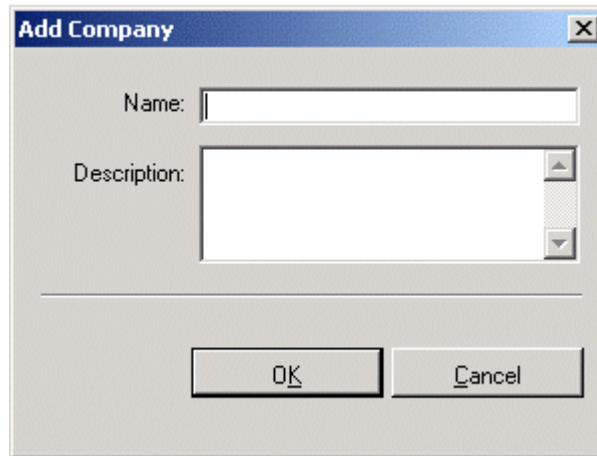
A dialog box titled "Add Company" with a close button (X) in the top right corner. It contains two input fields: "Name:" with a text box and "Description:" with a larger text area. At the bottom, there are two buttons: "OK" and "Cancel".

Figure 273: Adding a company

2. Enter a name and description.
3. To save the new company, click **OK**.

Modifying a Company

To modify a company, proceed as follows:

1. In the **Companies** window, select a company.
2. Double click the company, or click **Modify**.



The **Edit Company** window appears.

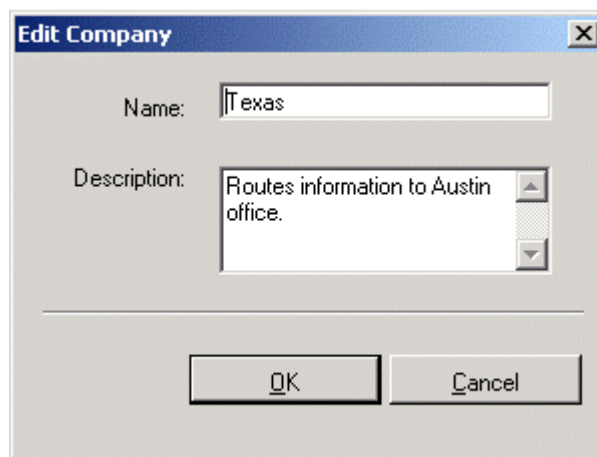
A dialog box titled "Edit Company" with a close button (X) in the top right corner. It contains two input fields: "Name:" with a text box containing the word "Texas" and "Description:" with a larger text area containing the text "Routes information to Austin office." At the bottom, there are two buttons: "OK" and "Cancel".

Figure 274: Modifying a company

3. In the **Name** and **Description** fields, enter appropriate values.

4. To save your changes, click **OK**.

Deleting a Company

To delete a company, proceed as follows:

1. In the **Companies** window, select a company.
2. Click **Delete**.



A confirmation window appears.

3. To delete the company, click **Yes**.
4. To cancel your request, click **No**.

Note: You cannot delete a company that is already associated with a form in E-Capture Definition Utility. If this is the case, an error message appears.

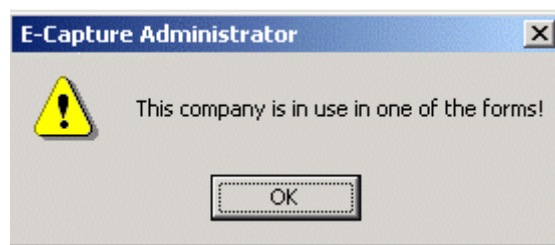


Figure 275: Company error message

Using E-Capture Custom Scripts

E-Capture processes documents without scripts, but scripts can be added as auxiliary tools. Scripts can be implemented to customize E-Capture.

The following topics are included in this section:

- [Overview](#)
- [Setting Up and Running E-Capture Custom Scripts](#)
- [Script Example](#)
- [Registering Scripted Modules](#)
- [Registering Scripts](#)

Overview

E-Capture custom scripts are created using widely supported scripts that are compatible with Windows, such as Visual Basic, JavaScript, and Perl.

An E-Capture script is a text file with a corresponding file extension. E-Capture compatible file extensions are described in the following table:

E-Capture compatible script file extensions	
Script type	File extension
Visual Basic	.vbs
JavaScript	.js
Perl	.pl

If a ScriptCall is registered in E-Capture Administrator, E-Capture Definition Utility or E-Capture Server processes files until it detects a ScriptCall. When it detects the ScriptCall, the script assigned to the ScriptCall continues the process. The script receives input variables delivered by E-Capture Definition Utility or E-Capture Server, performs calculations, and returns output variables to E-Capture Definition Utility or E-Capture Server.

After finishing its tasks, the script returns control to E-Capture Definition Utility or E-Capture Server. They continue processing documents using output variables from the script.

Each script receives and returns common variables. This makes it possible to exchange information between scripts.

Each script receives information about the corresponding input document directory. This makes it possible for a script to process documents arriving from different sources.

E-Capture is delivered with predefined ScriptCalls that represent standard behavior. The default behavior is hard coded and cannot be changed without reprogramming the application.

Setting Up and Running E-Capture Custom Scripts

To set up and run E-Capture custom scripts, proceed as follows:

1. Request an appropriate script template from Exigen Professional Services.
2. Prepare a script file based on the template.
3. Register the module, E-Capture Definition Utility or E-Capture Server, in which custom scripts are used.
4. Register the required ScriptCall as described in [Registering ScriptCalls](#).
5. Assign the required script file to the corresponding ScriptCall as described in [Registering Scripts](#).
6. If working with E-Capture Server, select the **Use custom scripts** option.

For more information on the **Use custom scripts** option, see the *Exigen Workflow Administrator's Guide, Part 2: Business Component Reference*, Chapter 18: E-Capture Server, Adding a Directory Configuration.

Selecting the **Use custom scripts** option ensures that scripts are automatically called from E-Capture Definition Utility and E-Capture Server.

Script Example

In the following example, documents are processed as follows:

1. E-Capture Server processes PDF files.
2. The PDF file name is used as part of the index string.
3. The last 15 characters of the PDF file name are not required and are eliminated from the index string by using the following E-Capture custom scripts:

E-Capture custom scripts	
Script	Function
Transformfilename.vbs	Receives the file name and transforms it into a global variable.
TransformIndexRow.vbs	Receives the file name global variable, extracts the required characters from the file path, and replaces the index string with this information.

The following text is from the TransformIndexRow.vbs custom script:

```
*****
' Transformindexrow script allows transforming the
' original index string by using
' information that comes from sScriptGlobal

' The global and specific variables should not be declared

'Global variables.
'1. sPreprocessing ; Deliver information going from the external sources
'2. sScriptGlobal  ; Use for exchange between scripts
'3. sReturn        ; Use to return string
'4. nReturn        ; Use to return numeric value

' Specific variables
'1. sIndexRow      ; Delivers the original index row
'2. sDirectoryIn   ; Delivers the paths of the current input directory

'Body of the script
Dim N
Dim Y
Dim patrN
Dim DeletredRightCharacters
Dim regEx          ' Create variables.
```

```

DeletedRightCharacters=15
N = Len(sScriptGlobal)
If N > DeletedRightCharacters Then
    Y=Left(sScriptGlobal, N - DeletedRightCharacters)
Else
    Y="Unrecognized"
End If
patrn=sScriptGlobal
Set regEx = New RegExp      ' Creates regular expression.
regEx.Pattern = patrn       ' Sets pattern.
regEx.IgnoreCase = True     ' Makes case insensitive.
sScriptReturn = regEx.Replace(sIndexRow , Y)
                             ' Makes replacement.

```

Registering Scripted Modules

Exigen E-Capture provides the Registering Modules tool as a customization solution for installing and running custom scripts without changing basic E-Capture modules.

The **Registering Modules** tool is used to register software modules to which you want to assign custom scripts.

To register scripted modules, proceed as follows:

1. In the **Administrator** window, click **Registering Modules**.



The **Registering Modules** window displays a list of all registered modules.

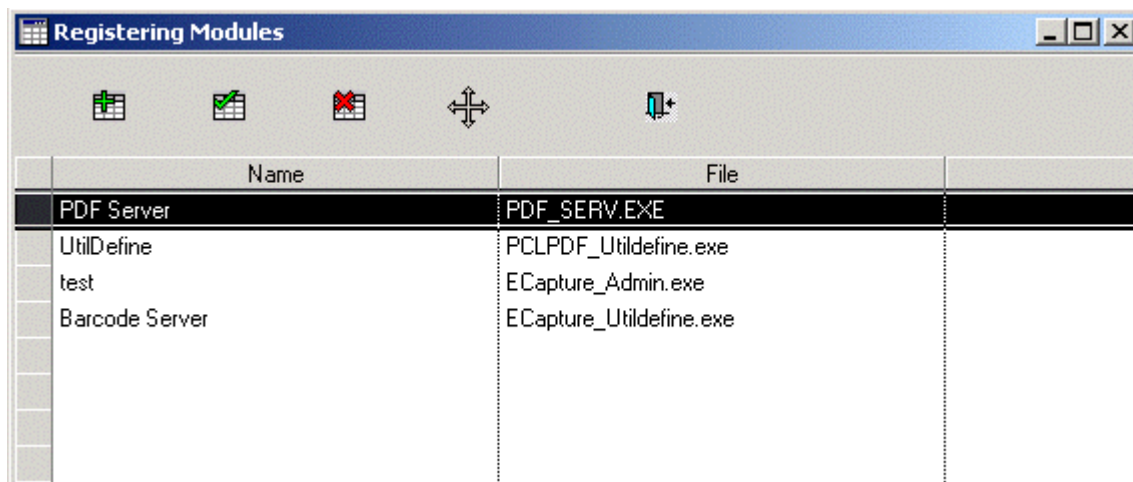


Figure 276: Registering scripted modules

2. Use the **Registering Modules** window to perform the following procedures:

- [Adding a Module](#)
- [Modifying a Module](#)
- [Deleting a Module](#)
- [Registering ScriptCalls](#)

Adding a Module

To add a scripted module, proceed as follows:

1. In the **Registering Modules** window, click **Add**.



The **Add Module** window appears.

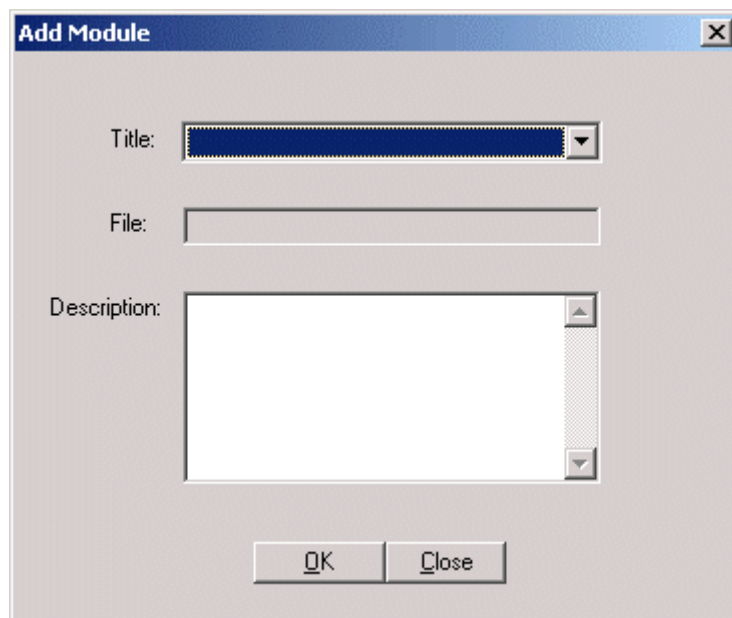


Figure 277: Add Module window

2. In the **Title** list box, select a module.

The module file name appears in the **File** field.

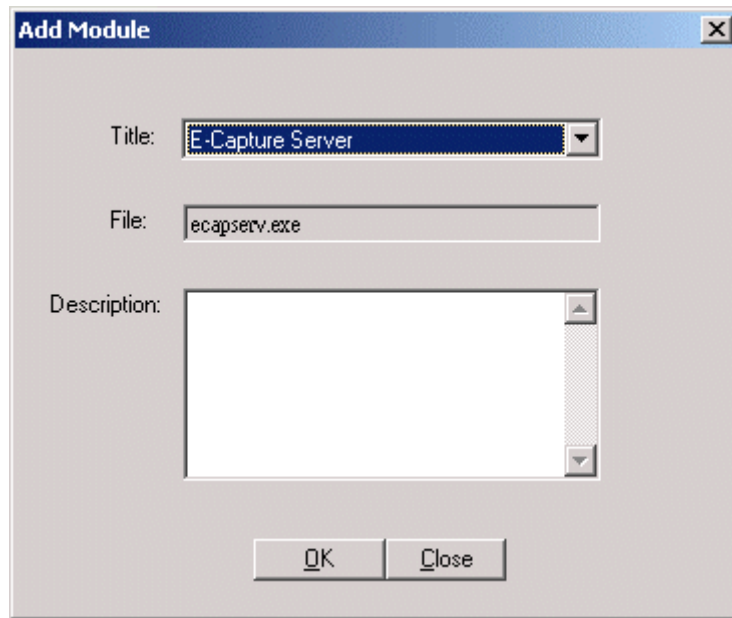


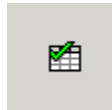
Figure 278: Selecting a source script file

3. In the **Description** field, enter a description.
4. To save the new registered module, click **OK**.

Modifying a Module

To modify a registered module, proceed as follows:

1. In the **Registering Modules** window, select a module.
2. Double click the module, or click **Modify**.



The **Modify Module** window appears.

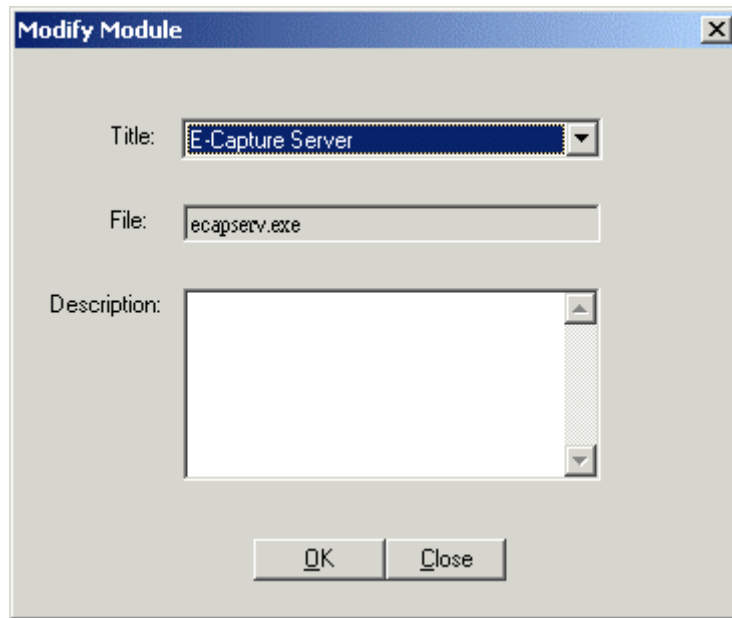


Figure 279: Modifying a scripted module

3. In the **Description** field, enter a description.
4. To save changes, click **OK**.

Deleting a Module

To delete a registered module, proceed as follows.

1. In the **Registered Modules** window, select a module.
2. Click **Delete**.



A confirmation window appears.

3. To delete the module, click **Yes**.
4. To cancel your request, click **No**.

Registering ScriptCalls

A ScriptCall is a special place in a software module that initiates a custom script. The **Details** tool is used to register the ScriptCalls to be used by each module. You must register ScriptCalls before you can register scripts. For information on how to register scripts, see [Registering Scripts](#).

For a description of supported ScriptCalls and their default behaviors, see [Appendix F: ScriptCalls](#).

To register ScriptCalls, proceed as follows:

1. In the **Registering Modules** window, select the module to which you want to assign a ScriptCall.

2. Click **Details**.



The **Registering Calls** window displays all registered ScriptCalls.

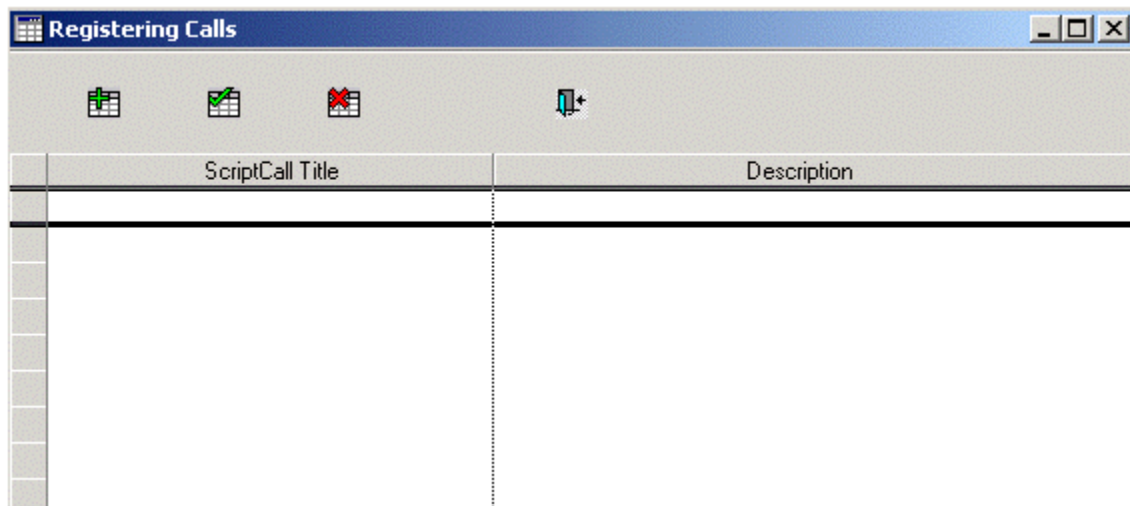


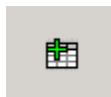
Figure 280: Registering ScriptCalls

3. Use the **Registering Calls** window to perform the following procedures:
 - [Adding a ScriptCall](#)
 - [Modifying a ScriptCall](#)
 - [Deleting a ScriptCall](#)

Adding a ScriptCall

To add a ScriptCall, proceed as follows:

1. In the **Registering Calls** window, click **Add**.



The **Add ScriptCall** window appears.

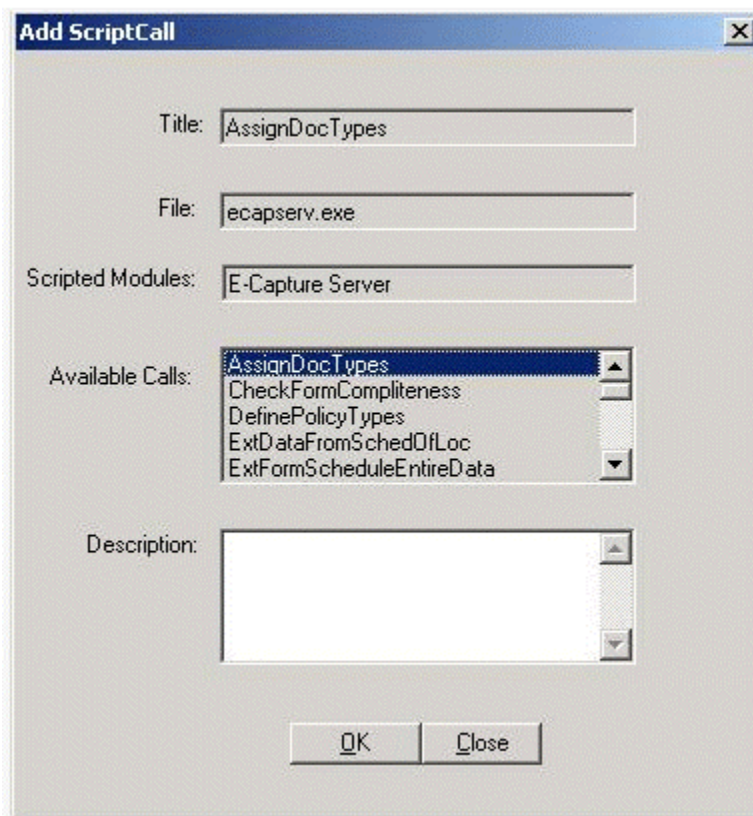


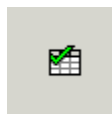
Figure 281: Adding a ScriptCall

2. In the **Available Calls** box, select a ScriptCall.
The selected ScriptCall appears in the **Title** field.
3. In the **Description** field, enter a description.
4. To save the new ScriptCall, click **OK**.

Modifying a ScriptCall

To modify a ScriptCall, proceed as follows:

1. In the **Registering Calls** window, select a ScriptCall.
2. Double click the ScriptCall, or click **Modify**.



The **Modify ScriptCall** window appears.

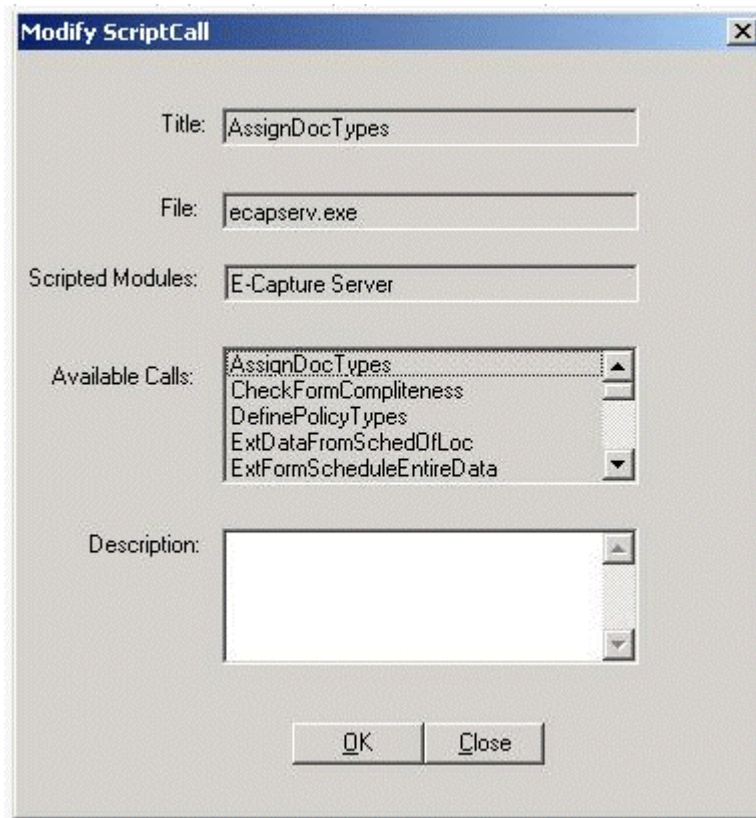


Figure 282: Modifying a ScriptCall

3. In the **Available Calls** and **Description** fields, enter appropriate values.
4. To save changes, click **OK**.

Deleting a ScriptCall

To delete a ScriptCall, proceed as follows:

1. In the **Registering Calls** window, select a ScriptCall.
2. Click **Delete**.



A confirmation window appears.

3. To delete the ScriptCall, click **Yes**.
4. To cancel your request, click **No**.

Registering Scripts

The **Script Maintenance** tool is used to register the scripts that you use to customize E-Capture. Scripts and templates must already be prepared.

To register scripts, proceed as follows:

1. In the **Administrator** window, click **Script Maintenance**.



The **Script Maintenance** window displays all registered scripts and attributes.

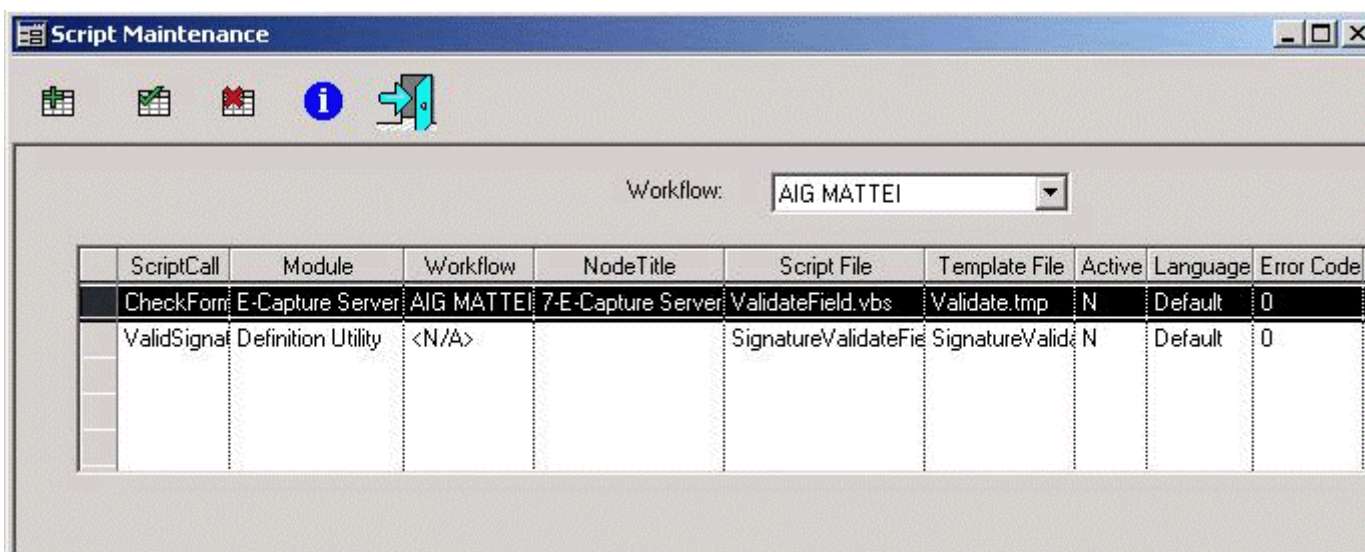


Figure 283: Registering scripts

The attributes of each registered script are described in the following table:

Script attributes	
Attribute	Description
Title	Registered ScriptCall name.
Module	Registered module name using the ScriptCall.
Node Title	Node name if the assigned module is a node in a workflow.
Workflow	Destination workflow name in which E-Capture files are placed.
Script File	File name and script extension.
Template File	File name and script extension's corresponding template file.
Active	Y if the ScriptCall is active, and N if not. If the ScriptCall is active, E-Capture executes it. If inactive, the ScriptCall is skipped.
Language	Script language type. Default refers to default script that cannot be changed.
Error Code	Numerical digit representing the binary code of error handling procedures configured in the Exceptions tab.

2. In the **Workflow** list box, to display all scripts previously registered, select the destination workflow name.
3. In the **Module** list box, to display scripts assigned to that particular module, select a registered module.


4. To display scripts assigned to all modules, select **<All>**.
5. Use the **Script Maintenance** window to perform the following procedures:
 - [Adding a Script](#)
 - [Modifying a Script Assignment](#)
 - [Deleting a Script Assignment](#)
 - [Viewing a Script's Properties](#)

Adding a Script

E-Capture obtains script and template files from the following default directory:

```
..EWF\SYSTEM\EcaptScripts
```

Before adding a script, ensure that the script and template files are located in this directory.

To add a script, In the **Script Maintenance** window, click **Add**  and enter values in the tabs as described in this section.

The **Assign New Script** window appears.

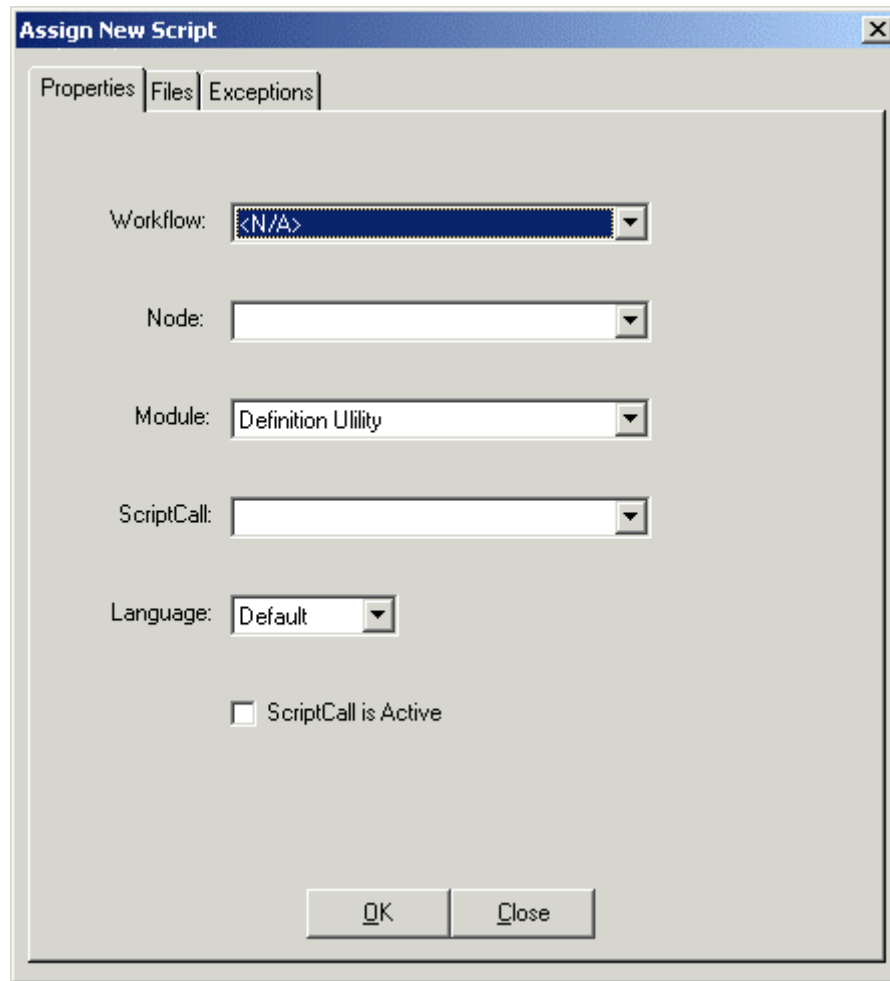


Figure 284: Assigning a new script, Properties tab

Use the **Properties**, **Files**, and **Exceptions** tabs to set properties for scripts as follows:

- [Properties Tab](#)
- [Files Tab](#)
- [Exceptions Tab](#)

Properties Tab

The **Properties** tab is used to specify general script attributes.

To specify general script attributes, proceed as follows:

1. In the **Workflow** list box, select the name of the destination workflow in which documents are placed. If the destination is not a workflow object, select **<N/A>**.
2. In the **Node** list box, select the name of the scripted workflow node.

If you are not using a workflow module, no choices are available for selection.

3. In the **Module** list box, select the module or workflow node to which you want to assign the new script.

4. In the **ScriptCall** list box, select the ScriptCall title.
5. In the **Language** list box, select the script language.

If you select **Default**, the E-Capture default procedure is used instead of the script.

6. To use E-Capture Server to execute the script, select the **ScriptCall is Active** check box.
7. To ignore the script, clear the check box.

Files Tab

The **Files** tab is used to select the script and template file sources.

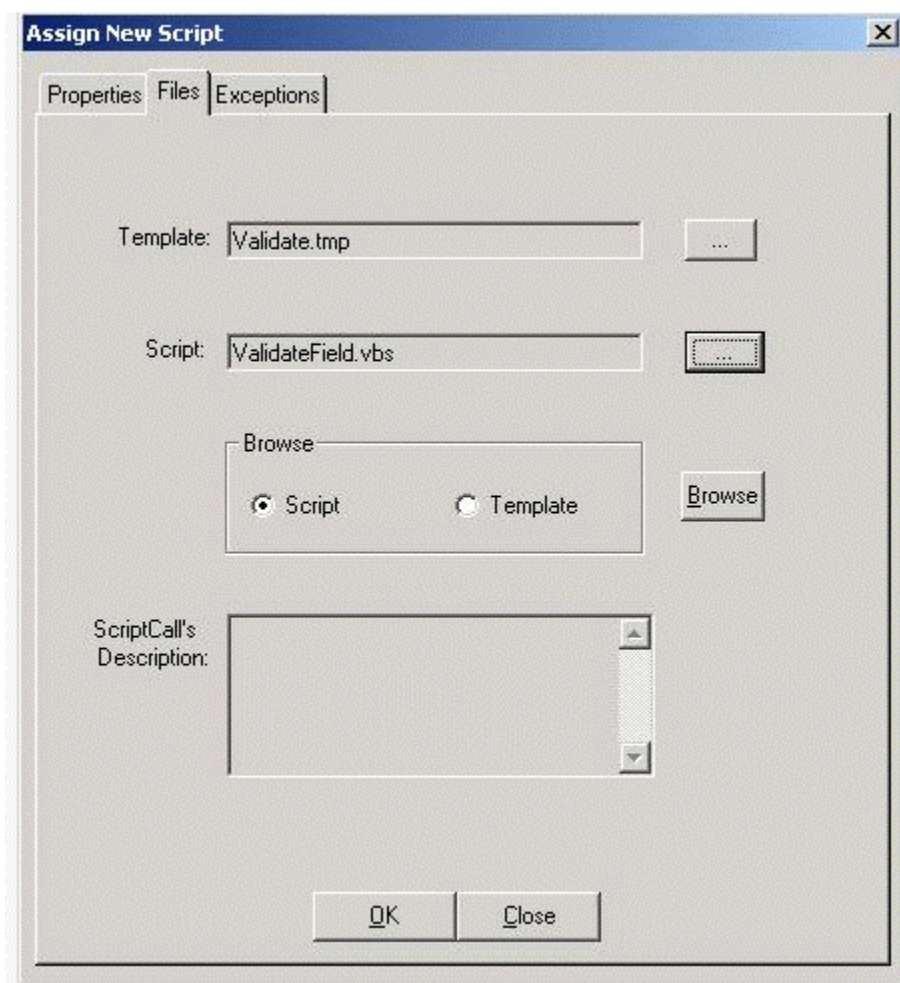


Figure 285: Selecting script and template file with Files tab

To view the script or template file, use the tools provided in the **Browse** panel.

- To view the file named in the **Script** field, select the **Script** radio button.
- To view the file named in the **Template** field, select the **Template** radio button.
- To view the named file, click **Browse**.

To select a source script file and a source template file, proceed as follows:

1. Click the browse button next to the **Template** field.

The **Open File** window appears.

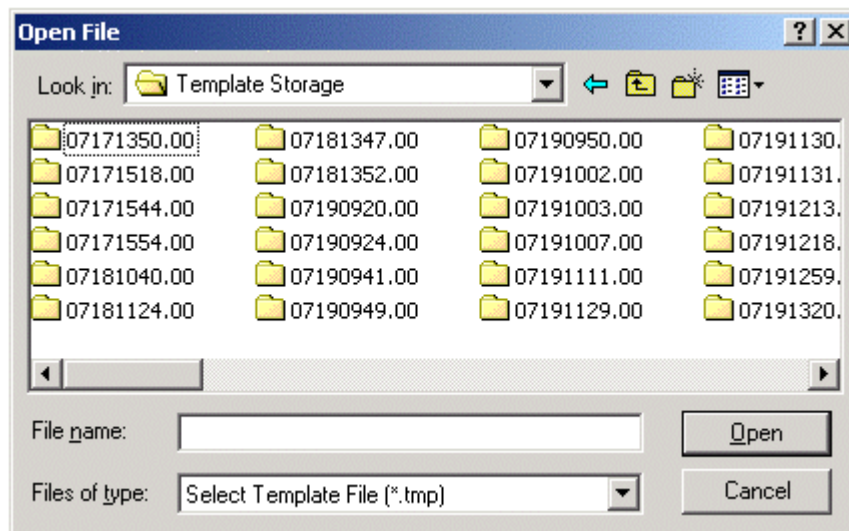


Figure 286: Browsing for template file

2. Select a file and click **Open**.

The name of the template file appears in the **Template** field.

3. Click the browse button next to the **Script** field.

The **Open File** window appears.

4. In the **Open File** window, select a script.

The script file name appears in the **Script** field.

Exceptions Tab

The **Exceptions** tab displays the four most common file processing errors encountered by E-Capture Server:

- Script file is not found.
- Wrong template is used.
- Error occurs during script execution.
- Wrong request is used.

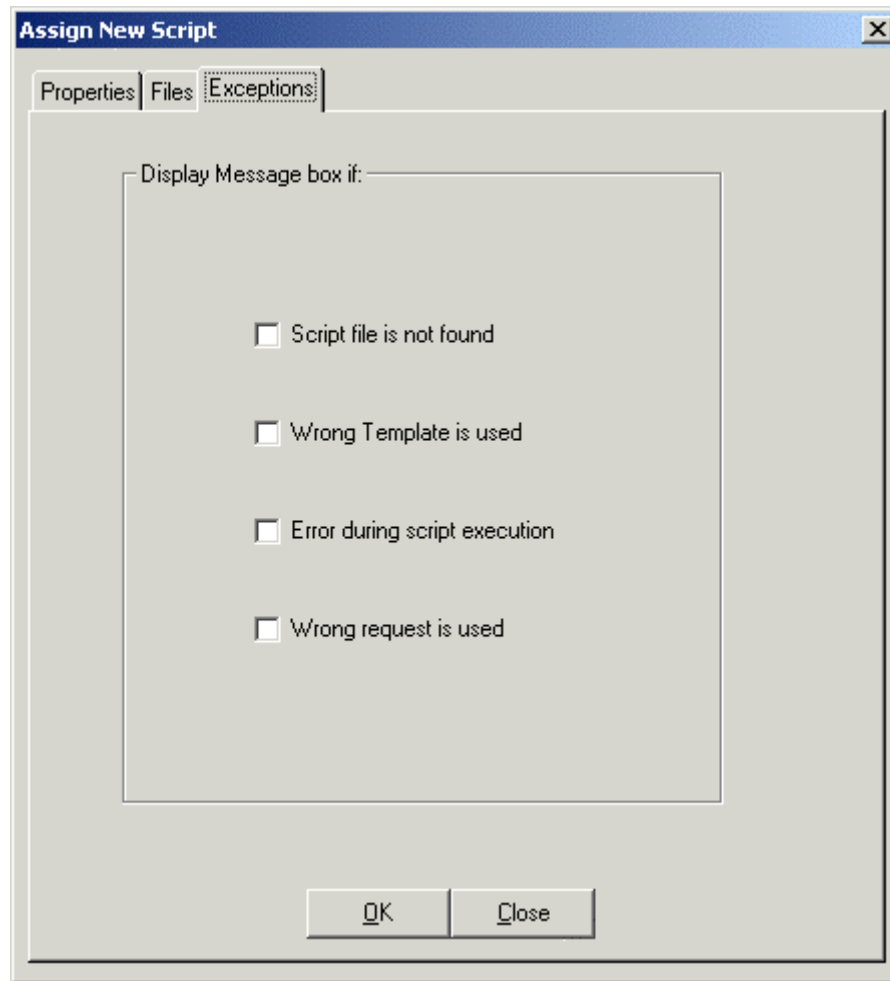


Figure 287: Using the Exceptions tab to configure error handling

To configure error handling, proceed as follows:

1. In the **Exceptions** tab, select the errors to be reported by E-Capture Server.
If a box is cleared, E-Capture Server does not report that error.
2. To save the new script assignment, click **OK**.

Modifying a Script Assignment

To modify a script assignment, proceed as follows:

1. In the **Script Maintenance** window, select a script.
2. Double click the script or click **Modify**.



The **Modify Script Assignment** window appears.

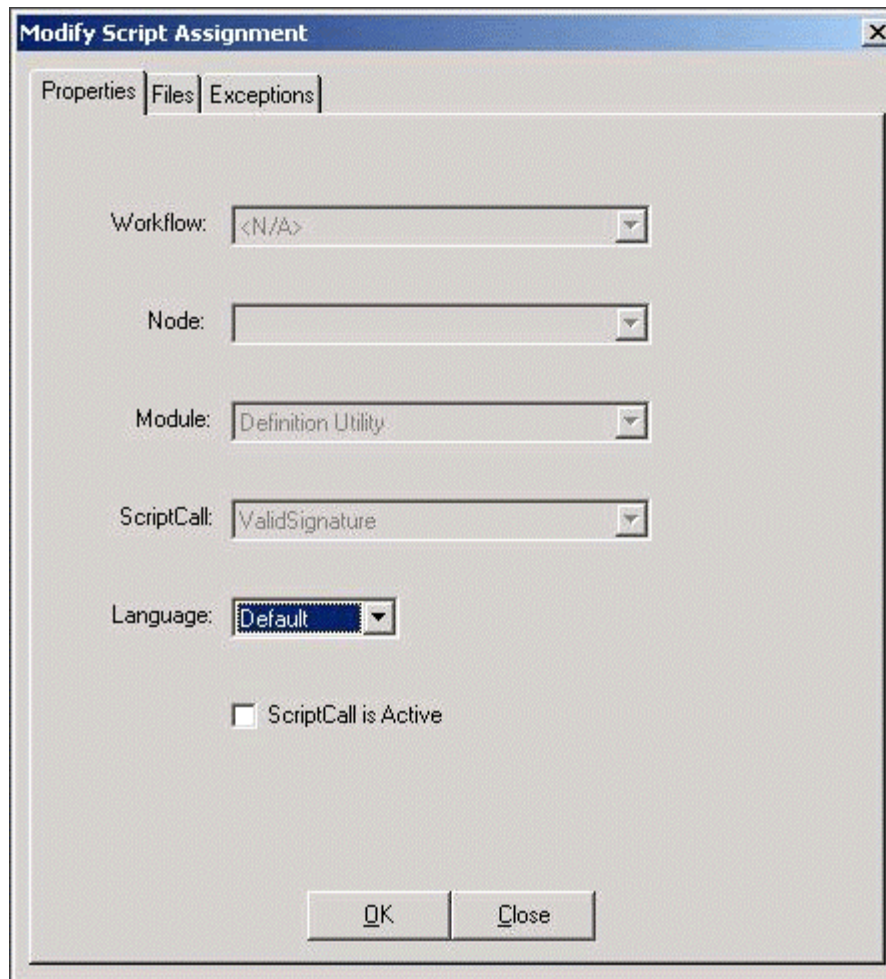


Figure 288: Modifying script assignment

3. Modify the settings in the **Properties**, **Files**, and **Exceptions** tabs as described in [Adding a Script](#).
4. To save changes, click **OK**.

Deleting a Script Assignment

To delete a script assignment, proceed as follows:

1. In the **Script Maintenance** window, select a script.
2. Click **Delete**.



A confirmation window appears.

3. To delete the ScriptCall, click **Yes**.
4. To cancel your request, click **No**.

Viewing a Script's Properties

To view general properties of a script assignment, proceed as follows:

1. In the **Script Maintenance** window, select a script.
2. Click **Info**.



The **ScriptCall Info** window appears.

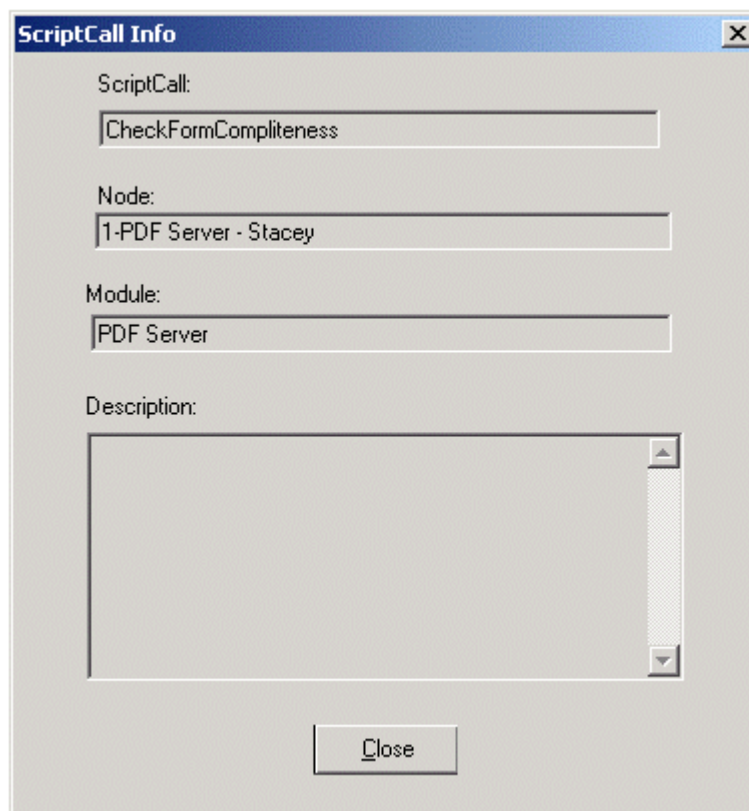


Figure 289: Viewing script properties

The **ScriptCall Info** window displays the name of the ScriptCall, the module, and Exigen Workflow node to which it is assigned.

3. To close the window, click **Close**.

Chapter 10: Setting Up User Synchronization Service

This chapter describes the user synchronization service (ADSync) and explains how to install, configure, and run it.

Note: ADSync is delivered as part of the Exigen Workflow installation package, but can also be purchased separately.

The following topics are described in this section:

- [Overview](#)
- [ADSync Functionality](#)
- [Logging Function](#)
- [Installing ADSync](#)
- [Configuring ADSync](#)
- [Registering and Running the ADSync Module](#)
- [Exigen Workflow Audit Events Generated by ADSync](#)
- [Setting up Exigen Workflow User Groups, Global User Groups, and Security Levels](#)
- [Integrating Integrated Security Management Console with ADSync](#)

Overview

ADSync is a service that retrieves and synchronizes user data so that users registered outside the Exigen Workflow system are not required to be registered individually by an Exigen Workflow administrator.

ADSync allows you to retrieve user information from an external source, such as Directory/Domain Service (DS) or Genesys Enterprise Routing Solution (ERS). Depending on the external source, users can be assigned particular privileges and restrictions not accorded to users registered solely as Exigen Workflow users.

For example, users from DS who successfully log in to a domain can log in to Exigen Workflow without a secondary authentication. Users from Genesys ERS can open tasks assigned to them by Genesys ERS through the Genesys Universal Agent Desktop without a secondary authentication in Exigen Workflow. It is possible to limit Genesys ERS users' access rights to this Genesys Universal Agent Desktop or to assign these users any access rights available for Exigen Workflow.

The ADSync module implements synchronization from DS and Genesys ERS to Exigen Workflow and to a database. This service synchronizes only users and their membership in groups, not the groups themselves. You can add and disable users and modify user group membership, but you cannot create or delete groups. You must still create groups manually through Exigen Workflow Administration Tools.

ADSync does not attempt to modify the workflow group, global user group, or security level of a user if the directory group specified as the synchronization source for the group or security level does not exist or is not accessible.

ADSync is implemented as a standard Windows NT service. Configuration information for this service is stored in the computer's registry. Except for database connection parameters, the service dynamically changes its configuration according to the registry settings. The service uses the Windows NT event log to report critical errors and other events. In addition, you can dynamically change the logging level as well as run ADSync in console mode, using the console window and log file for output.

ADSync retrieves user group and user information from any source that supports the required Active Directory Service Interfaces (ADSI)-compatible interfaces.

ADSync Functionality

User synchronization is a four-step process as follows:

1. ADSync synchronizes DS users with the Exigen Workflow database.

Users are created with the default settings from the Exigen Workflow group setup and the Users Synchronization Setup. The settings provided by the Exigen Workflow group setup are authentication modes and database user type. The default settings are set for all created users in Exigen Workflow and are never changed by ADSync. Other settings, such as a default password and force default password, are specified in the Users Synchronization Setup.

When a new Exigen Workflow user is created, ADSync assigns a password to the user. The following rules apply:

- If no password is provided by the DS, ADSync assigns a default password. Because Genesys ERS allows password information to be accessed, ADSync uses the password provided by Genesys ERS.
- If a password is provided by the DS, and the **Force default password** option is not enabled, the provided password is assigned to the user. ADSync assigns the password without verifying whether it complies with Exigen Workflow password requirements.
- If a password is provided by the DS, and the **Force default password** option is enabled, the default password is assigned to the user.

The following rules apply when user information is updated:

- If the DS provides a password and the **Force default password** option is enabled, the default password is assigned to the user.
- If the DS provides a password and the **Force default password** option is not enabled, the DS password is assigned to the user. ADSync assigns the password without verifying whether it complies with Exigen Workflow password requirements.
- If the DS does not provide a password, the existing password remains unchanged.
- If the system administrator changes the default password, all passwords provided by the DS are updated automatically for all synchronized users.

The default password is intended to be temporary. It is recommended that the user change the default password to a new password when first logging in to Exigen Workflow.

2. ADSync synchronizes workflow user groups and global user groups.

For more information on workflow user groups and global user groups, see [Setting up Exigen Workflow User Groups, Global User Groups, and Security Levels](#).

3. ADSync synchronizes user security levels.

ADSync assigns the default security level for all newly created users. This level can be changed as required if synchronization information is entered in the **Security Level Setup** dialog in Exigen Workflow Administrator. ADSync assigns the given security level to all Exigen Workflow users imported from the specified DS group. Further modifications of the user's security level are not required, unless the Exigen Workflow administrator changes the user's security level back to the default value used by ADSync.

4. ADSync synchronizes Exigen Workflow users with the database and synchronizes database user role membership.

The database user type of the Exigen Workflow user is stored in the `DB_USER_TYPE` field in the `S01_USERS` table. ADSync exports any synchronized Exigen Workflow user to the database if this field contains values 1– standard or 2 – windows. In case of a Windows user, `LOGIN_DOMAIN` must contain a valid domain name.

In the **Security Level Setup** dialog in Exigen Workflow Administrator, you can specify a database role to which all users with the given Exigen Workflow security level are added. If `Administrators` is selected in the `Database Role` field, all synchronized database users are added to `vfadmins` for SQL and Oracle databases and `db_owner` database roles and `Security Administrators` fixed server role for SQL databases only. If `Users` is selected, users are added to `vfusers` role.

ADSync does not delete users from the Exigen Workflow database because Exigen Workflow users may have assigned parcels, tasks, and other Exigen Workflow objects. Deleting users is the administrator's responsibility. Instead, ADSync disables any synchronized Exigen Workflow user if this user was removed from all Exigen Workflow groups.

Note: If the system administrator set **Value by AdSync** in the **Password** tab as described in [Specifying the Authentication Mode](#), ADSync alone determines whether the user can log in to Exigen Workflow. Group member synchronization takes place without regard for the account status set by the administrator.

Note: Within the Exigen Workflow database, all user names are uppercase. When synchronizing, all user names are written in this manner. For example, John and JohN in Windows become the same user, JOHN, in Exigen Workflow.

ADSync synchronizes only users whose user names consist of alphanumeric characters. If you attempt to synchronize a user whose name contains non-alphanumeric characters, the following message appears:

The user will not be added to Exigen Workflow database. Invalid USER_ID.

Logging Function

The log is written as follows to different sections of the event log depending on the version of Windows used:

- If ADSync is installed on Windows NT 4.0 and is run as a service, it writes to the `Applications` section of the event log.

- If ADSync is installed on Windows 2000 or Windows XP and is run as a service, it writes to the `ADSync` section of the event log.

Depending on the log level, if ADSync is started as a console, it displays logged information in the console. If the log is to be written to the console and to a file, the file name must be indicated along with the command line switches, as in the following example:

```
ADSync.exe -debug log.txt
```

The file is saved in the current directory or in a specified directory.

Installing ADSync

The following topics are described in this section:

- [System Requirements](#)
- [Installation](#)

System Requirements

ADSync has the same system requirements as Exigen Workflow. For information on Exigen Workflow system requirements, see the Exigen Workflow readme file.

To start ADSync, Administrator access rights are required. If ODBC is used, access rights for the required ODBC DSN must be configured.

Installation

To install ADSync, proceed as follows:

1. Run the Exigen Workflow installation CD.
2. In the **Optional Components**, select **User Synchronization (ADSync)**.
3. If you installed ADSync using the setup of Exigen Workflow or Universal Workflow Link, skip this step. To register ADSync as a service, in the command line, enter `ADSync.exe -install`.

The ADSync command switches are described in [Registering and Running the ADSync Module](#).

4. To configure ADSync, perform one of the following steps:
 - In the `EWF/SYSTEM` directory, run the `ADSyncSetup.exe` file.
 - In Exigen Workflow Explorer, select **Administration Tools > Workflow Tools > Users Synchronization Setup**.

The **Users Synchronization Setup** window appears.

5. Configure ADSync.

For information on configuring ADSync, see [Configuring ADSync](#).

6. Click **Save**.

7. Click **Start Service**.

Configuring ADSync

Configuring ADSync requires knowledge of the following topics:

Required knowledge for configuring ADSync	
Topic	Website for additional information
Windows script technologies	http://msdn.microsoft.com/library/default.asp?url=/library/en-us/dnanchor/html/scripting_a.asp
ADSI	http://msdn.microsoft.com/library/en-us/adsis/adsis/active_directory_service_interfaces_adsi.asp?frame=true
ADSI extensions	http://msdn.microsoft.com/library/en-us/adsis/adsis/adsis_extensions.asp?frame=true

A familiarity with COM aggregation is also recommended. For information on COM aggregation, see the following website:

http://msdn.microsoft.com/library/en-us/adsis/adsis/revisiting_com_aggregation_rules_with_adsi_extensions.asp?frame=true

The following topics are included in this section:

- [Synchronization with Directory Services](#)
- [Connecting to a Database Using OLE DB](#)
- [Configuring ADSync and Mapping a Directory Service](#)
- [Exposing Internal ADSync Objects For Use in Mapping Scripts](#)
- [Mapping Examples](#)

Synchronization with Directory Services

ADSync supports synchronization with a variety of directory services, including Active Directory®, iPlanet, WinNT, and GCDI. Names and syntaxes of the attributes required for creating a valid Exigen Workflow user account differ for various directory services.

The following topics are included in this section:

- [IEWFExtension Interface](#)
- [ADSI Extensions for Exigen Workflow Architecture](#)
- [Mapper Object Overview](#)
- [Extensions for ADSI User Group Objects](#)
- [Extensions for ADSI User Objects](#)

IEWFExtension Interface

To synchronize with directory services, ADSync and the ADSI extensions for Exigen Workflow must be configured correctly. ADSync always uses the IEWFExtension interface for accessing directory services. The IEWFExtension interface provides a standard way of accessing directory data. Attributes required for Exigen Workflow user records are mapped from a directory services object to appropriate fields in the Exigen Workflow database.

As part of the ADSync configuration process, a mapper object is configured for access to directory services. The mapper object translates directory service attribute names to Exigen Workflow field names and returns the value associated with the field name.

ADSI Extensions for Exigen Workflow Architecture

ADSI extensions for Exigen Workflow are implemented as COM objects. The IEWFExtension interface is registered by the system administrator as an extension for the required ADSI class instance. ADSI automatically handles initialization of the extension object using COM aggregation. The security context of the IEWFExtension instance is the same as for ADSI itself.

When initialized, the IEWFExtension instance performs the following tasks:

1. Gets the provider and class names of the aggregator.
2. Composes a ProgID of a predefined mapper object using the following syntax:
`"EWFExtension.<ADSIProviderName>.<ADSIClassName>."`

This ProgID is unique for the given workstation.

3. Instantiates the mapper object of the given ProgID and initializes it.

Mapper Object Overview

The mapper object is a standard COM object supporting a dual interface. It must implement a single property accessor method: "Extends". This property is set to the ADSI object that aggregates the IEWFExtension instance. Windows Scripting is used to implement mapping objects. For information on scripting, see [Mapping Examples](#).

Extensions for ADSI User Group Objects

An ADSI user group is a container with an array of user objects. ADSync attempts to retrieve a "USER_ID" property for every group object accessed on the path retrieved from the Exigen Workflow database.

The variant returned by the extension must be a two-dimensional array containing a valid Exigen Workflow user ID, which is an alphanumeric string, in its first dimension, and a valid ADSI path to the appropriate user object in its second dimension.

For an example of a WinNT group extension, see [WinNT Group Object Extension Example](#).

Extensions for ADSI User Objects

ADSI paths returned in the array are used to access the appropriate ADSI user objects. The extension for ADSI user objects must be configured before using ADSync. For configuration information, see [WinNT User Object Extension Example](#).

It is possible to specify the S01_USERS table fields that can be synchronized. To do this, the ADSI user extension must contain attributes with names that match the required S01_USERS field names. The following field names are automatically filled in by ADSync, while ADSI values are overridden:

- LOGIN
- CUR_BARCODE
- SYNC_MODE
- USER_DIS_AS
- USER_DISABLED
- LEVEL_ID

USER_ID is a mandatory attribute, and is used for validation purposes.

If the field names ALLOW_AUTH_MODES, AUTH_MODE, and DB_USER_TYPE are specified in a script, but a script attribute value is not assigned, the value is the default set during workflow groups setup, and the value is not updated.

For example, if the ALLOW_AUTH_MODES value is not set, but ALLOW_AUTH_MODES is specified as a synchronized field, when a user is created, the field value is the default specified during workflow group setup. When the user is updated because another workflow or global group contains this user, the ALLOW_AUTH_MODES value does not change.

If the **Force default password** option is set when configuring ADSync, the PAROLE value is overridden and the default password is used.

If the **Use upper case for Workflow user data** option is set when configuring ADSync, string conversions are performed by ADSync for the following fields:

- USER_ID
- LOGIN
- CUR_BARCODE

Connecting to a Database Using OLE DB

To connect to a database using OLE DB, perform the following preliminary steps before configuring ADSync:

1. In the `visi.ini` file, create a new section:

```
[OLE_DB_<DB_NAME_ALIAS>]  
constring=<DB_CONNECTION_STRING>;
```

<DB_NAME_ALIAS> must be a database alias and must be identical to the DBS_MASTER value in the [databases] section of the `visi.ini` file.

<DB_CONNECTION_STRING> must be a valid OLE DB connection string.

For example, enter the following:

```
[OLE_DB_visiop]  
constring=Provider=SQLOLEDB;Server=austin;Database=visiop;
```

2. Ensure that the OLE DB connection string does not include the database user name and password.

The user name and password are derived from the [databases] section for the respective database name alias.

3. Save and close the visi.ini file.

Configuring ADSync and Mapping a Directory Service

This section describes the following procedures to configure ADSync and map a directory service:

- [Starting Users Synchronization Setup and Connecting to a Database](#)
- [Configuring ADSync](#)
- [Configuring a Mapper Object](#)

Starting Users Synchronization Setup and Connecting to a Database

To start Users Synchronization Setup and connect to a database, proceed as follows:

1. In Exigen Workflow Explorer, select **Administration Tools > Workflow Tools > Users Synchronization Setup**.

The **Users Synchronization Setup** window appears.

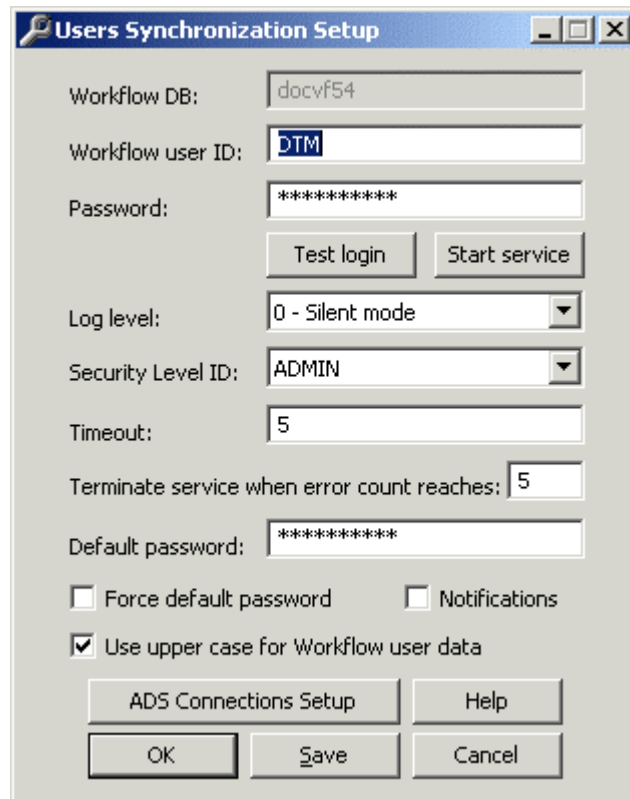


Figure 290: Setting up ADSync

If a user name and password are required, the **Users Synchronization Setup** login window appears.

2. To connect to a database, enter your user name and password and click **Connect**.
3. In the **Users Synchronization Setup** window, in the **Workflow user ID** field, enter your Exigen Workflow user name.
4. In the **Password** field, enter your Exigen Workflow password.

ADSync uses the same user name and password for database access.

Note: The database connection must be established by a database user who has administrative rights for the current database and is a member of the Security Administrators fixed server role for the SQL server. For more information on access rights, see [Appendix G: Exigen Workflow User Authentication Mechanism](#).

5. To ensure that the user name and password are correct, click **Test login**.

If these parameters are not correct, the following message appears:



Figure 291: Users Synchronization Setup message

When ADSync is running, the **Stop service** button appears by default.

6. To stop ADSync, click **Stop service**.

Once the service is stopped, the **Start service** button replaces the **Stop service** button.

7. To start the ADSync module, click **Start service**.

Configuring ADSync

To configure ADSync, proceed as follows:

1. Enter appropriate data in the following fields:

- **Log level**
- **Security Level ID**
- **Timeout**
- **Default Password**

For information on the preceding fields, see the following table:

ADSync configuration parameters	
Parameter	Description
Log level	<p>Determines the logging level of ADSync:</p> <ul style="list-style-type: none"> • 0 = silent mode, in which the file is not created • 1 = errors only • 2 = actions that modify the database like Add or Delete User • 4 = all actions like Find Users Group • 6 = all SQL statements issued • 8 = debug mode
Security Level ID	System-wide level ID used when a new Exigen Workflow user is added. The default level is ADMIN.
Timeout	Time interval in seconds between ADSync activation periods. The recommended timeout for 100 agents is 6 seconds to 9 seconds, depending on the system speed.
Terminate service when error count reaches	Number of errors after which the service is stopped automatically. These can be database connection or exception handling errors. Automatic restart is available only if it is configured in the Windows Services manager.

ADSync configuration parameters	
Parameter	Description
Default password	<p>String assigned to users retrieved from Genesys ERS and Directory/Domain Service (DS).</p> <p>If the default password does not comply with Exigen Workflow security settings, an error message is displayed, and the user is not able to log in to Exigen Workflow.</p> <p>For information on specifying password security settings, see Specifying Security Settings.</p>
Force default password	<p>If this check box is selected, all the Genesys agents who are synchronized with the Exigen Workflow system have the default password assigned. If cleared, the password string is the same as in the Genesys system for Genesys users, and empty for DS users.</p>
Notifications	<p>Option is available only for Genesys ERS. It is not available for Windows DS.</p> <p>GCDI notifications are issued only when user information is updated. When user information is modified at run-time, only updates for the modified users are committed to the database.</p> <p>This option has the following possible values:</p> <ul style="list-style-type: none"> • Cleared: ADSync does not attempt to establish notification listening on any of the requested DS groups. • Selected: ADSync attempts to establish notification listening on all of the requested DS groups. If the attempt is successful, no synchronization with the groups listened to, except at startup, is done unless a notification arrives. Groups with no notification listening are synchronized depending on timer settings.
Use upper case for Workflow user data	<p>Uppercase letters are used for Exigen Workflow data.</p>

2. Select other options as described in the preceding table.
3. If you require a connection to a DS group outside the current domain, to specify a user name and password for this connection, proceed as follows:
 - Click **ADS Connection Setup**.

The **ADS Connections Setup** window appears.

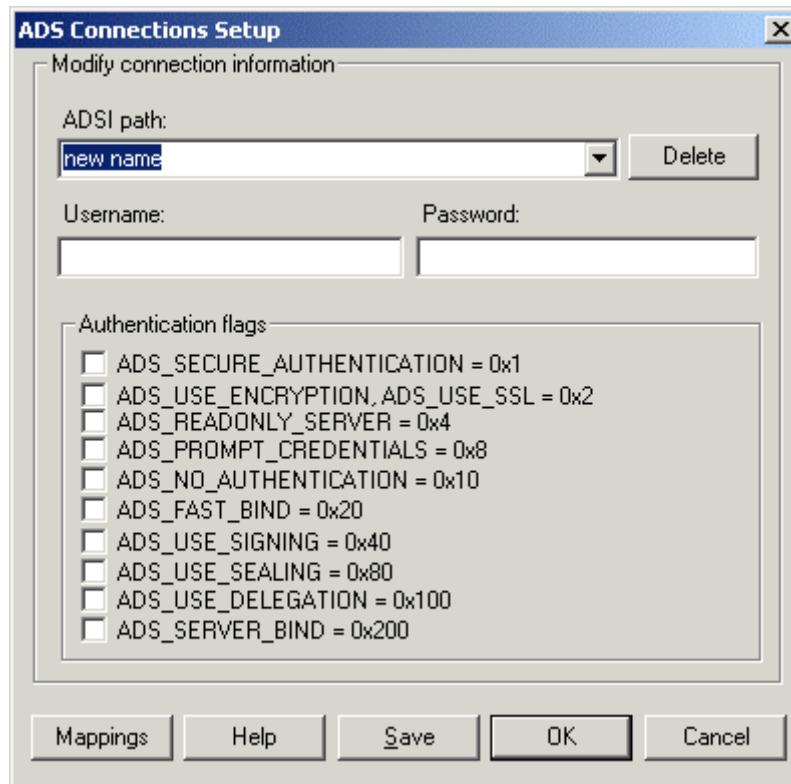


Figure 292: Setting up a connection

- In the **ADS Connections Setup** window, in the **ADS path** field, specify the path to the group outside the domain. Alternatively, specify the part of the path that is identical for all domain objects or the distinguished name (DN) of the domain.
- If you manually entered the name of a connection path, click **Add**.
- To delete a selected connection path, click **Delete**.
- In the **Username** field, enter an optional user name.
- In the **Password** field, enter a password.

A password is entered only if the user name has a password associated with it.

- To specify authentication flags, in the **Authentication flags** section, select at least one option.

Authentication flags are used as parameters for the `ADsOpenObject` function to retrieve directory data.

For more information on authentication options, see the following website:

http://msdn.microsoft.com/library/en-us/adsi/adsi/ads_authentication_enum.asp?frame=true

Configuring a Mapper Object

To configure a mapper object for synchronization with directory services, proceed as follows:

1. Click **Mappings**.

If the connection is successful, the **ADSI to EWF Mappings Setup** window appears.

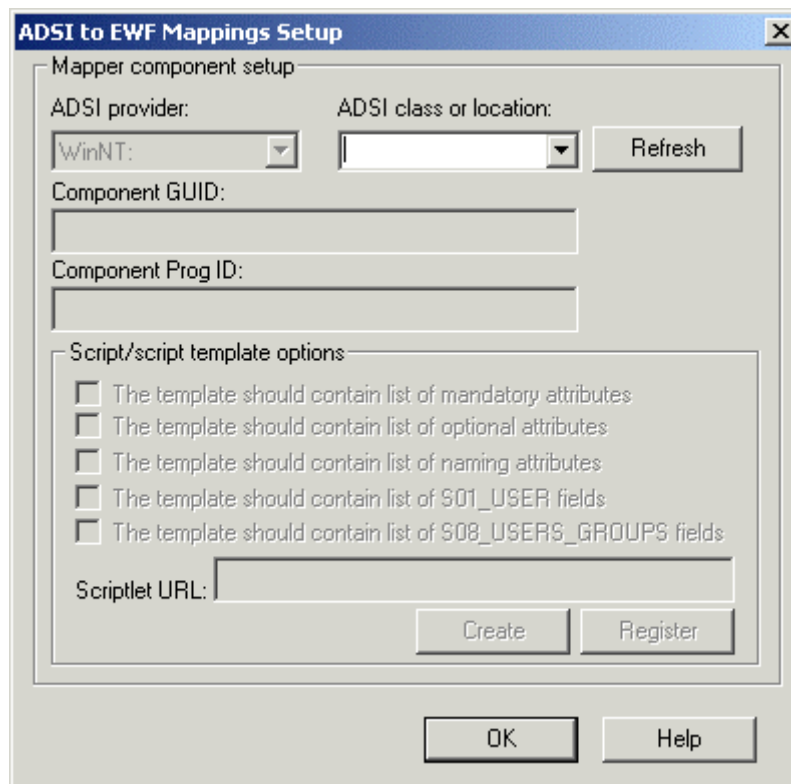


Figure 293: Configuring a mapper object

If the connection is not successful, an error message appears that describes the possible cause of the failure.

2. To specify an ADSI provider, in the **ADSI provider** field, select a provider.
3. To select a class to map, in the **ADSI class or location** field, select or enter a class or class location.

For information on predefined scripts for classes, see [Mapping Examples](#).

4. To update the **Component GUID** and **Component Prog ID** fields, click **Refresh**.

The Component GUID is assigned automatically for each new mapper component.

The ProgID is generated as follows:

```
"EWFExtension.<ADSI Provider Name>.<Class Name>"
```

If the class is not found, the class or location is incorrect, and an error message appears.

5. If an incorrect class or location was entered, in the **ADSI class or location** field, select the correct class or location.
6. To specify script options, In the **Script/script template options** section, select appropriate options.

The **Scriptlet URL** field displays the file name or path to the scriptlet describing the mapper object.

7. To create the script, click **Create**.

The script appears.

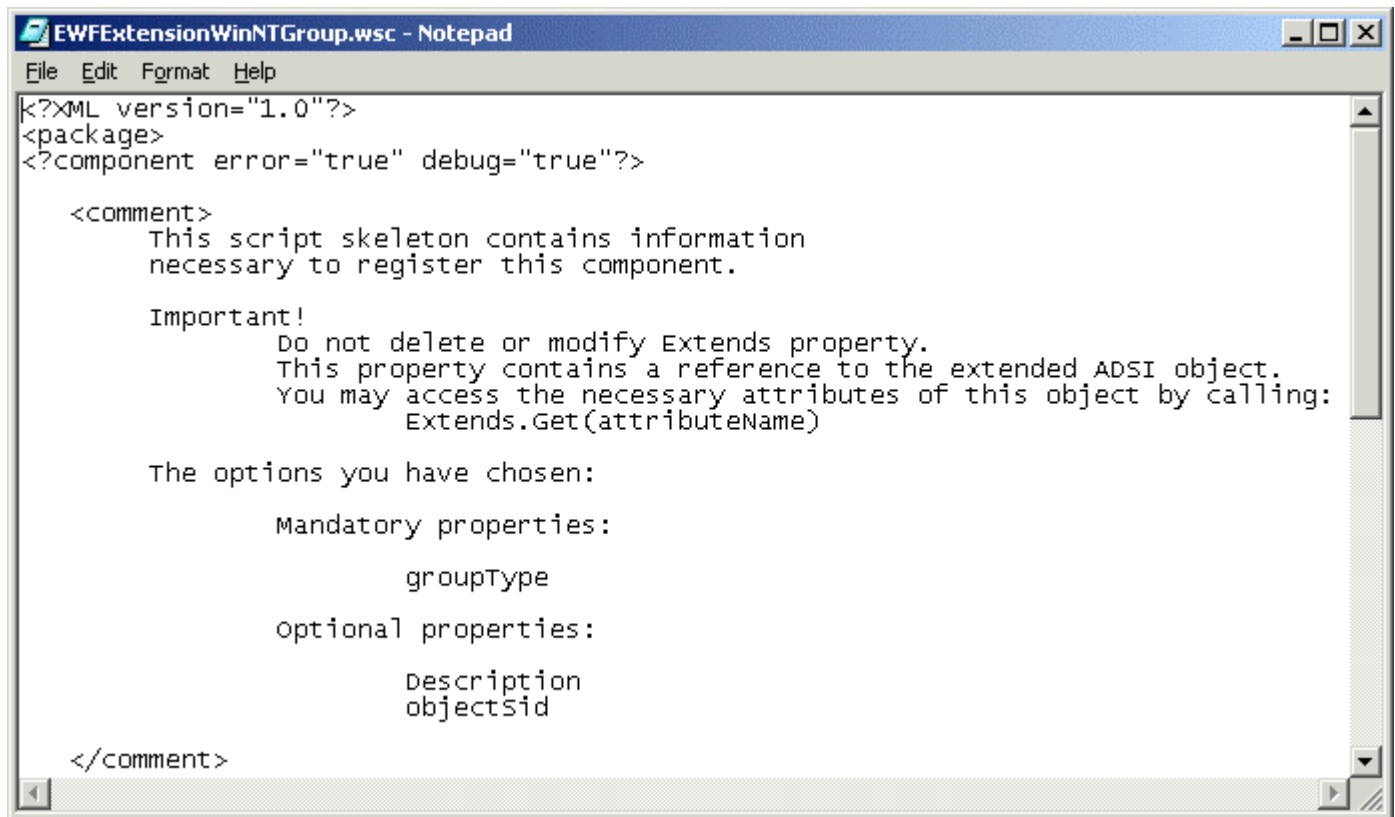


Figure 294: Defining a mapping object script

8. In the script, enter mandatory values.

For information on mandatory values, see [Mapping Examples](#).

9. To register the script, click **Register**.

When the script is registered, a notification appears.

10. To view a script created previously, click **View**.
11. To unregister a non-GCDI script that is no longer required, click **Unregister**.
12. To unregister a GCDI script that is no longer required, in Windows Explorer, right click the script file and select **Unregister**.
13. To close the window, click **OK**.
14. In the **Users Synchronization Setup** window, to save the changes and close the window, click **OK**.
15. To save the changes without closing the window, click **Save**.
16. To close the window without saving, click **Cancel**.

When starting ADSync for the first time, synchronization is performed. Thereafter, the synchronization starts after notification for groups with synchronization enforced, or every time, as specified in the

Timeout field, for groups without notifications enforced. A whole synchronization loop is performed each time.

The following table describes possible access rights:

ADSync access rights			
Default Password is not empty	Force default password check box is selected	Exigen Workflow administrator assigned the password manually	Access to Exigen Workflow using the standard Exigen Workflow Login window
X	X		All Genesys agents with default password.
	X		No Genesys agents.
	X	X	Only Genesys agents configured in the Exigen Workflow database.

Exposing Internal ADSync Objects For Use in Mapping Scripts

ADSync is capable of exposing the following internal objects to the ADSI Extension:

- ADSI object that actually calls the specified extension
- ADODB connection object that allows access to the master database

To allow ADSync exposure to the extended ADSI object, the script must have the following property:

```
<property name="IsObjectExtended"/>
```

The default value of the property is `False`. To expose the extended object, set this property to `True` as follows:

```
dim IsObjectExtended
IsObjectExtended=True
```

If `IsObjectExtended` is set to `True`, ADSync initializes the `Extends` property with an ADSI object that invoked this ADSI extension. Otherwise, the `Extends` property is initialized with the ADSI path to the extended object.

To allow ADSync to expose the master DB connection object, the script must have the following property:

```
<property name="MasterDBConnection"/>
```

When the extension script is called, ADSync initializes the `MasterDBConnection` property with an ADODB connection object that is connected to the same database that ADSync.

Mapping Examples

The following topics are included in this section:

- [Mapping Scripts Supplied with ADSync](#)
- [WinNT Group Object Extension Example](#)
- [WinNT User Object Extension Example](#)

Mapping Scripts Supplied with ADSync

The most commonly used classes have scripts that are supplied with the ADSync installation. The following table lists the mapping scripts supplied with ADSync:

Mapping scripts supplied with ADSync		
Provider	Class	File name
WinNT	User	EWFExtensionWinNTUser.wsc
WinNT	Group	EWFExtensionWinNTGroup.wsc
LDAP	group	EWFExtensionLDAPgroup.wsc
LDAP	groupOfNames	EWFExtensionLDAPgroupOfNames.wsc
LDAP	inetOrgPerson	EWFExtensionLDAPinetOrgPerson.wsc
LDAP	person	EWFExtensionLDAPperson.wsc
LDAP	user	EWFExtensionLDAPuser.wsc
LDAP	ePerson	EWFExtensionLDAPePerson.wsc

The files are viewed or registered by selecting the class name for the given provider in the **ADSI to EWF Mappings Setup** window in the **ADSI class or location** field. Files must be registered manually. For information on the **ADSI to EWF Mappings Setup** window, see [Configuring ADSync and Mapping a Directory Service](#).

WinNT Group Object Extension Example

The following is an example of a WinNT group object extension:

```
<?XML version="1.0"?>
<package>
<?component error="true" debug="true"?>
  <comment>
    This script skeleton contains information
    required to register this component.

    Important!
    Do not delete or modify the Extends property.
    This property contains the ADSI path to the extended ADSI object.
    You may access the necessary attributes of this object by calling:
      Set object = GetObject(Extends)
      value = object.attributeName

    The options you have chosen:

  </comment>
<component id="EWFExtension.WinNT.Group">

  <registration
    progid="EWFExtension.WinNT.Group"
    description="Extends WinNT: Group class for Exigen Workflow ADSync"
    version="1"
    clsid="{FB1DDEC2-CCC1-46B2-8634-FFD8CC082A01}"
```

```

/>

<comment>
    "USER_ID" property is used by ADSync to access directory group
    contents.
</comment>

<public>
    <property name="Extends"/>

    <property name="USER_ID">
        <get internalName = "get_USER_ID"/>
    </property>
</public>

<script language="VBScript">

    '"Extends" property is set by ADSI Extensions for Exigen Workflow when
    the ADSI object
    'of the specified class is created.
    dim Extends
    Function get_USER_ID()
        '"USER_ID" property accessor must return a two dimensional array
        'containing USER_ID field value in its first dimension and exact ADSI
        path to user object in its second dimension.
        Dim ret()
        Dim idx
        Dim member
        Dim obj
        on error resume next
        Set obj = GetObject(Extends)
        For Each member In obj.Members
            'For WinNT provider, "Members" collection contains ADSI user
            'objects that are members of the specified group.
            'WinNT directory can have nested groups (i.e., groups can be
members
            'of other groups). Member's class must be checked:
            if member.Class="User" then
                ReDim Preserve ret(1,idx)
                'member's name and ADSI path are assigned to the respective
                'array elements:
                ret(0,idx)=member.Name
                ret(1,idx)=member.ADsPath
                idx=idx+1
            End if
            Set member=nothing
        Next
        Set member=nothing
        Set obj = nothing
        get_USER_ID = ret
    End Function
</script>

```

```
</component>
</package>
```

WinNT User Object Extension Example

The following is an example of a WinNT user object extension:

```
<?XML version="1.0"?>
<package>
<?component error="true" debug="true"?>

  <comment>
    This script skeleton contains information
    required to register this component.

    Important!
    Do not delete or modify the Extends property.
    This property contains the ADSI path to the extended ADSI object.
    You may access the necessary attributes of this object by calling:
        Set object = GetObject(Extends)
        value = object.attributeName

    The options you have chosen:

  </comment>

<component id="EWFExtension.WinNT.User">

  <registration
    progid="EWFExtension.WinNT.User"
    description="Extends WinNT: User class for Exigen Workflow ADSync"
    version="1"
    clsid="{399723AA-6D46-448B-B4BC-A46F25B6EEBA}"
  />

  <public>

    <property name="Extends">
      <put internalName = "put_Extends"/>
      <get internalName = "get_Extends"/>
    </property>
    <property name="AUTH_MODE"/>
    <property name="ALLOW_AUTH_MODES"/>
    <property name="USER_NAME">
      <get internalName = "get_username"/>
    </property>
    <property name="DB_USER_TYPE"/>
  </public>

  <script language="VBScript">
```

```

        "Extends" property is set by ADSI Extensions for Exigen Workflow when
        the ADSI object of the specified class is created.
dim Extends
dim AUTH_MODE
dim DB_USER_TYPE
dim USER_NAME
Function put_Extends(val)
    on error resume next
    Extends = val
    Dim obj
    Set obj = GetObject(Extends)
    'Assign default values to mandatory Exigen Workflow fields
    'AUTH_MODE = "V" - Workflow authentication is the default
    AUTH_MODE = "V"
    'ALLOW_AUTH_MODES = "V;" - allow only workflow authentication
    ALLOW_AUTH_MODES = "V;"
    'DB_USER_TYPE = 0 - user does not have direct database access
    DB_USER_TYPE = 0
    'LOGIN_DOMAIN - iterates up the directory tree to find the domain of
    'the current user. This functionality is not available to all servers.
    dim parent
    set parent=obj
    while Not parent.Class = "Domain"
        set parent = GetObject(parent.Parent)
    wend
    LOGIN_DOMAIN = parent.Name
    Set obj = Nothing
End Function

Function get_Extends
    get_Extends = Extends
End Function

Function get_username
    'USER_NAME (person's name) property is assigned in this function.
    'Checking is performed for empty FullName property - Exigen
Workflow does not
    'allow users with empty names.
    On error resume next
    Dim obj
    Set obj = GetObject(Extends)
    if obj.FullName = "" then
        get_username=obj.Name
    Else
        get_username=obj.FullName
    End if
    Set obj = Nothing
End Function

</script>
</component>
</package>

```

Registering and Running the ADSync Module

To register and run the ADSync module after preliminary steps are complete, proceed as follows:

1. To launch the ADSync module, run the `ADSync.exe` file.
2. Use the following command switches:

Command switches	
Switch	Description
<code>- install</code>	Registers the service. EventLog output.
<code>- remove</code>	Unregisters the registered service. EventLog output.
<code>- debug</code>	Runs in continuous mode. Console output.
<code>- step</code>	Runs one synchronization loop. Console output. Exigen Workflow users are created based on directory service users.
<code>- check</code>	Runs one consistency-check loop and one synchronization loop. Console output.
<code>- dbsync</code>	Runs one synchronization loop. Console output. Database users are based on Exigen Workflow users.
<code>- logfile_name</code>	Writes console output to this file.

The synchronization loop consists of the following:

- synchronization of users for each non-empty SYNC_INFO in the table S05_GROUPS.
- synchronization of users' Level_ID for each non-empty SYNC_INFO in the table S03_LEVELS.
- synchronization of Exigen Workflow users with database and synchronization of database role membership.

The synchronization loop is performed in the following cases:

- when the timeout elapses
- when a GCDI notification on added or deleted users is received

The consistency-check loop consists of the following:

- synchronization loop
- determining for each synchronization group in the table S05_GROUPS that each record in the table S08_USERS_GROUPS is valid, that is, the user exists in the table S01_USERS

A consistency check loop is performed in the following cases:

- on startup
- after Force Default Password and Default Password values are changed in the registry
- GCDI notification on changes of a listened DS group or deletion of the group arrives
- user name value of a user in any group listened to changes

Customizing Exigen Workflow

The field SYNC_INFO in the tables S03_LEVELS and S05_GROUPS must either contain valid Active Directory paths to the group object, or they must be empty.

Examples

For Windows NT:

```
WinNT://DTMX/Group
```

where

WinNT is the Windows NT namespace; also works in Windows 2000.

DTMX is the domain name.

Group is the group name in domain.

Users can log in to Exigen Workflow using an automatic logon only from the domain specified in this path.

For Genesys ERS:

```
GCDI://GenConfServer/Configuration/Resources/Agent Groups/VF1
```

where

GCDI is the Genesys Configuration Directory Interface.

GenConfServer is the Genesys Configuration Server alias specified when setting up GCDI using UWL Configuration Tool.

Resources is the tenant.

Agent Groups is the group container.

VF1 is the agent group name.

Note: During the synchronization process, the security level of the group is assigned automatically to all new users in this group.

For more information on security levels in the S03_LEVELS table, see [Specifying Security Levels](#). For information on using UWL Configuration Tool, see the *Universal Workflow Link Configuration Guide*.

Exigen Workflow Audit Events Generated by ADSync

ADSync generates Exigen Workflow audit events. To ensure that these events are audited, an audit project must be created as described in [Creating a New Project](#). The audited events appear in the Exigen Workflow audit log.

The following table describes Exigen Workflow audit events generated by ADSync:

Exigen Workflow audit events generated by ADSync
--

Message ID	Description
10340	Exigen Workflow user is created.
10342	Exigen Workflow user is modified.
10343	User security level is changed.
10347	User account is disabled.
10348	User is enabled.
10404	Database server login is created or access is granted to a Windows NT user.
10406	Database server login is not created or access is not granted to a Windows NT user.
10408	Database server login is deleted or access is removed for a Windows NT user.
10410	Database server login is not deleted or access is not removed for a Windows NT user.
10412	Database user is created or access is granted for a Windows NT user.
10414	Database user is not created or access is not granted for a Windows NT user.
10416	Database user is deleted or access is removed for a Windows NT user.
10418	Database user is not deleted or access is not removed for a Windows NT user.
10420	Database user is added to the specific database role.
10422	Database user is not added to the specific database role.
10424	Database server login is added to the specific database server role.
10426	Database server login is not added to the specific database server role.
10438	User is added to the Exigen Workflow group.
10440	User is removed from the Exigen Workflow group.
10446	User is added to global group.
10448	User is removed from global group.

For more information about the preceding events, see [Audit Event Descriptions](#). For more information about the Exigen Workflow audit function, see [Chapter 11: Using Audit Log Viewer](#) and [Appendix D: Audit Data in Exigen Workflow](#).

Setting up Exigen Workflow User Groups, Global User Groups, and Security Levels

Each user group has a dialog that displays synchronization information, which is the path to the directory service group containing the list of users. During group setup, default parameters must be assigned to all new users. These default parameters apply only to new users. For more information on setting up Exigen Workflow user groups, see [Setting Up Workflow Groups](#).

Each global user group can be synchronized with an external directory service group. To synchronize a global user group with an external directory service group, synchronization information must be entered for each global user group to be synchronized. For more information on setting up Exigen Workflow global user groups, see [Setting Up Global User Groups](#).

If a global user group is assigned the **Automatically maintain this group** option, it is updated automatically based on filters defined by the administrator. Automatically maintained global user groups are updated by ADSync when any of the following conditions is fulfilled:

- if ADSync adds a new user to the Exigen Workflow database
- if ADSync modifies user information in the Exigen Workflow database
- if ADSync disables or enables a user

If both synchronization information and a filter are specified for a global user group, ADSync imports users into the Exigen Workflow database for that global user group, but only users matching the filter are added to the global user group. Users not matching the filter are disabled in the Exigen Workflow database if they are not members of any other workflow group or global user group.

If a new user is added to a global user group, all required security attributes for this user, such as database user type and authentication mode, must be specified in the mapping script. For information on mapping scripts, see [Mapping Examples](#).

When setting up a security level, the path to the directory group containing the list of users to be assigned to this security level must be specified.

If Exigen Workflow extended security is used, a database security role can be specified. Users are assigned to this role. For more information on database security, see [Specifying Security Levels](#).

User-Level Security

Security level synchronization is a different process from user synchronization because Exigen Workflow implements user-level security, that is, any user can have any security level. An unlimited number of security levels is allowed, and each level can have different permissions.

Modifying the Security Level

When ADSync creates new users in Exigen Workflow, it assigns a default security level to them as part of the users synchronization process.

To modify the security level, proceed as follows:

1. To specify different security levels for different user groups, enter the same synchronization information in the security level setup and the workflow group setup for any given user group.

For information on setting up a security level, see [Specifying Security Levels](#).

2. To specify the same security level for several workflow or Directory/Domain Service (DS) groups, use either of the following methods:
 - In Exigen Workflow, proceed as follows:
 - Create the required number of security levels, with identical properties but different names.
 - In the **Security Level Setup** dialog, point each security level to a different workflow or DS group by specifying the path to the group in the **Synchronization info** field.
 - In a Genesys or WinNT DS, proceed as follows:
 - Create a user group including all users to be assigned a single security level.
 - Point the security level to the new user group.

Example 1

Assume Exigen Workflow users are assigned to process jobs in Queue 3. Some of the users are allowed to edit document images, but some are not. The administrator creates the following two security levels for Exigen Workflow user group Q3:

- Q3EDIT
- Q3READ

Users are imported from the following WinNT domain group:

```
WinNT://COMPANY/Q3Users
```

The default security level is Q3READ. To assign a new security level to the users of Exigen Workflow group Q3 who are allowed to edit images, the administrator specifies the following for Q3EDIT:

```
WinNT://COMPANY/ImageEditors
```

For Q3READ, no new assignment is required.

Example 2

In the following example, security levels are assigned for several user groups.

The following are WinNT user groups and users:

```
WinNT://Scanners
```

```
Scan1
```

```
Scan2
```

```
Scan3
```

```
WinNT://QueueReaders
```

```
QRead1
```

```
QRead2
```

```
QRead3
```

```
WinNT://QueueEditors
```

```
QEdit1
```

```
QEdit2
```

```
QEdit3
```

```
WinNT://Others
```

```
Other1
```

```
Other2
```

```
Other3
```

The following are Exigen Workflow user groups:

```
SCAN with synchronization information: WinNT://Scanners
```

```
QREAD with synchronization information: WinNT://QueueReaders
```

```
QEDIT with synchronization information: WinNT://QueueEditors
```

```
OTHERS with synchronization information WinNT://Others
```

The following are Exigen Workflow security levels:

```
SCAN LEVEL with synchronization information: WinNT://Scanners
```

```
QREAD LEVEL with synchronization information: WinNT://QueueReaders
```

QEDIT LEVEL with synchronization information: WinNT://QueueEditors
 USERS without synchronization information and limited permissions

The default level specified by the ADSync setup is USERS .

The following table describes the resulting security levels for Exigen Workflow users:

Exigen Workflow users, user groups, and security levels		
Exigen Workflow user ID	Exigen Workflow user group	Exigen Workflow security level
SCAN1	SCAN	SCAN LEVEL
SCAN2	SCAN	SCAN LEVEL
SCAN3	SCAN	SCAN LEVEL
QREAD1	QREAD	QREAD LEVEL
QREAD2	QREAD	QREAD LEVEL
QREAD3	QREAD	QREAD LEVEL
QEDIT1	QEDIT	QEDIT LEVEL
QEDIT2	QEDIT	QEDIT LEVEL
QEDIT3	QEDIT	QEDIT LEVEL
OTHER1	OTHERS	USERS
OTHER2	OTHERS	USERS
OTHER3	OTHERS	USERS

Note: Users with no security level synchronization information specified are in the default security level.

Integrating Integrated Security Management Console with ADSync

The following topics are described in this section:

- [Overview](#)
- [Customizing Exigen Workflow](#)
- [Exigen Security Services Elements Collection Plug-in](#)

Overview

Exigen Security Services provides policy storage on the LDAP enabled Directory Server. The Exigen Security Services policy item privilege can be used as the synchronization access point in Directory Services. The **Integrated Security Management Console (ISMC)** is used to manage resources and user assignments. ISMC can be used to create policy resources, for example, document types. The privilege is used to identify which user has access to a specific resource, for example, document type.

The following figure shows how the ADSync script is used to retrieve the document type information:

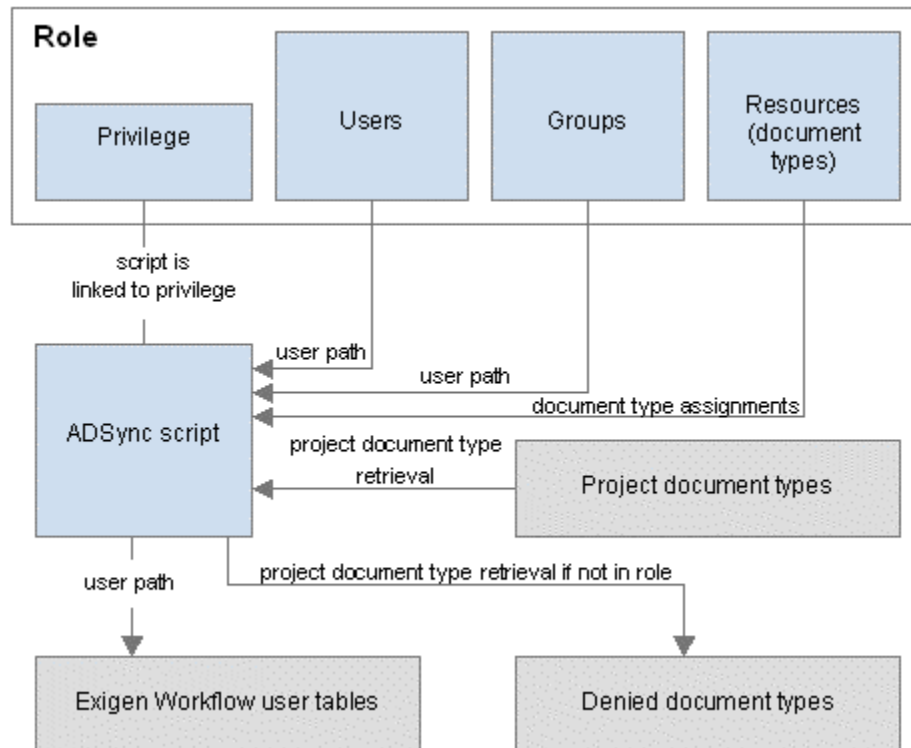


Figure 295: ADsync script receiving document type information

The ADsync script uses the privilege as an access point to process users, groups, and resources so that all document types that are not in the role are marked as not accessible for the users in the role.

For more information on ISMC, see the *ISMC Administrator's Guide*, which is available in the ISMC installation package.

Customizing Exigen Workflow

To integrate ISMC with ADsync, Workflow groups must be customized and the DN path to a privilege must be defined. The DN path can be obtained in the policy domain by inspecting the policy set. For example, privilege Use doctype can be found at the following LDAP location:

```
ldap://ADDEVDC.addev.exigengroup.lv/CN=Resource_Use%doctype_<someid>,CN=policySet,OU=Policy,DC=addev,DC=exigengroup,DC=lv.
```

Exigen Security Services Elements Collection Plug-in

The following topics are described in this section:

- [Exigen Security Services Elements Collection Installation Files](#)
- [Creating an Instance of the Exigen Security Services Elements Collection Plug-in](#)
- [Setting the Exigen Security Services Elements Collection Plug-in Username and Password](#)
- [Initializing the Exigen Security Services Elements Collection](#)
- [Specifying the Unique Identifier](#)

- [Retrieving the Assigned Document Types](#)
- [Uninitializing the Exigen Security Services Elements Collection](#)
- [EWFExtensionLDAPxacmlPolicy.wsc Script Helper Functions](#)

Exigen Security Services Elements Collection Installation Files

To access user and document type assignments information stored in an XACML policy set, a specially designed ADSync plug-in, the Exigen Security Services Elements Collection plug-in, must be used. This plug-in is included in the User Synchronization ISMC support package that is located in the following directory:

Windows\UserSynchronISMCSupport

The Exigen Security Services Elements Collection plug-in installs the following files in the Exigen Workflow system directory:

- EWFExtensionLDAPxacmlPolicy.wsc
- Xacml.core.dll
- SEAElementsCollection.dll

The EWFExtensionLDAPxacmlPolicy.wsc and Xacml.core.dll files contain the main functionality. The EWFExtensionLDAPxacmlPolicy.wsc script uses properties and methods that the plug-in exposes.

Creating an Instance of the Exigen Security Services Elements Collection Plug-in

To create an instance of the Exigen Security Services Elements Collection plug-in, the CreateObject method is used. The following is the method syntax:

```
Dim sea
Set sea = CreateObject("Visiflow.SEAtoEWF.SEAPolicySet")
```

After the instance is created, the appropriate properties must be initialized as described in [Setting the Exigen Security Services Elements Collection Plug-in Username and Password](#).

Setting the Exigen Security Services Elements Collection Plug-in Username and Password

To access the Directory Service from where the Exigen Security Services Elements Collection Plug-in retrieves its policy set information, a username and password can be required.

To set username and password, set the following properties:

```
username = "CN=AdminAD,CN=Users,DC=addev,DC=exigengroup,DC=lv"
password = "ActiveDir"
```

Initializing the Exigen Security Services Elements Collection

To initialize the Exigen Security Services Elements Collection with the required xacmlPolicySet, which provides all necessary user and document type assignment information, proceed as follows:

1. Call the Initialize method with the extended ADSI object as a parameter.

The syntax of the Initialize method is as follows:

```
sea.Initialize varExtends
```

2. Ensure that the extended ADSI object is an ISMC privilege with a valid xacmlPolicyID and xacmlXML properties.
3. To ensure that the extended ADSI object is an ISMC privilege, use the ADSI Browser tool `adsvw.exe` that can be downloaded from the following location:

<http://www.microsoft.com/ntserver/nts/downloads/other/ADSI25/default.asp>

Specifying the Unique Identifier

In ISMC, document types are stored as resources, each having a unique path. For example, assume there are three document types for the project that must be synchronized:

- TYPE_1
- TYPE_2
- TYPE_3

The document types have the following common identifier in the path:

```
/resources/doctypes/project_PRJ_doctypes/
```

To make these document type resources available in the Exigen Security Services Elements Collection, this unique identifier must be specified.

To specify the unique identifier, assign the following property:

```
sea.DefaultDocTypeIdentifier="/resources/doctypes/project_PRJ_doctypes/"
```

All document types in the policy set that are assigned to the synchronized privilege and contain the specified path are returned as an array of strings when the next function is called.

Retrieving the Assigned Document Types

When all initialization steps succeed, a list of users, their respective ADSI paths, and the document types that are assigned to each user within the returned list can be retrieved using the following method:

```
Dim users
```

```
Dim paths
```

```
Dim doctypes
```

```
sea.GetPriviledgeUsersAndDoctypes users, paths, doctypes
```

Uninitializing the Exigen Security Services Elements Collection

When the work with Exigen Security Services Elements Collection is finished, uninitialize the Exigen Security Services Elements Collection as follows:

Set sea=Nothing

EWFExtensionLDAPxacmlPolicy.wsc Script Helper Functions

The EWFExtensionLDAPxacmlPolicy.wsc script contains the following helper functions that can be adjusted to the specific needs as described in the following table:

EWFExtensionLDAPxacmlPolicy.wsc script helper functions	
Function	Description
CreateArrayFromUsersAndPaths	Creates an array from the list of users and ADSI Paths. CreateArrayFromUsersAndPaths function takes an array of users and an array of ADSI paths returned by GetPrivilegedUsersAndDoctypes function, and returns a two dimensional array that can later be passed back to ADSync for processing.
AssignDoctypes	Removes all document type assignments for all users that are returned in the list, and denies access to document types for the specified users.
DenyDoctypesAccessForUsers	Takes a list of users and a list of document types as parameters and creates the entries in the S10_USER_DOCTYPE table. Users are denied access to these document types.
GetDoctypeProject	Gets a list of projects where the specified doctype id is found. The parameter for this function is doctype id.
IsDoctypeInProject	Checks whether the specified project_id_DOCTYPE table contains the specified doctype. The function is used by the GetDoctypeProject function.
DeleteProjectDoctypeUser	Deletes a row with a matching project id, user id, and a doctype from the S10_USER_DOCTYPE table.
InsertProjectDoctypeUser	Inserts a row with a matching project id, user id, and a doctype in the S10_USER_DOCTYPE table.

Chapter 11: Using Audit Log Viewer

Exigen Workflow Audit Log accumulates changes made in the system. The data that appears in this log is specified by audit filters. For more information on audit filters, see [Defining Audit Filters](#).

To view the audit log content, sort, and filter records, in **Workflow Tools**, double click **Audit Viewer**.



The **Audit Log Viewer** window appears.

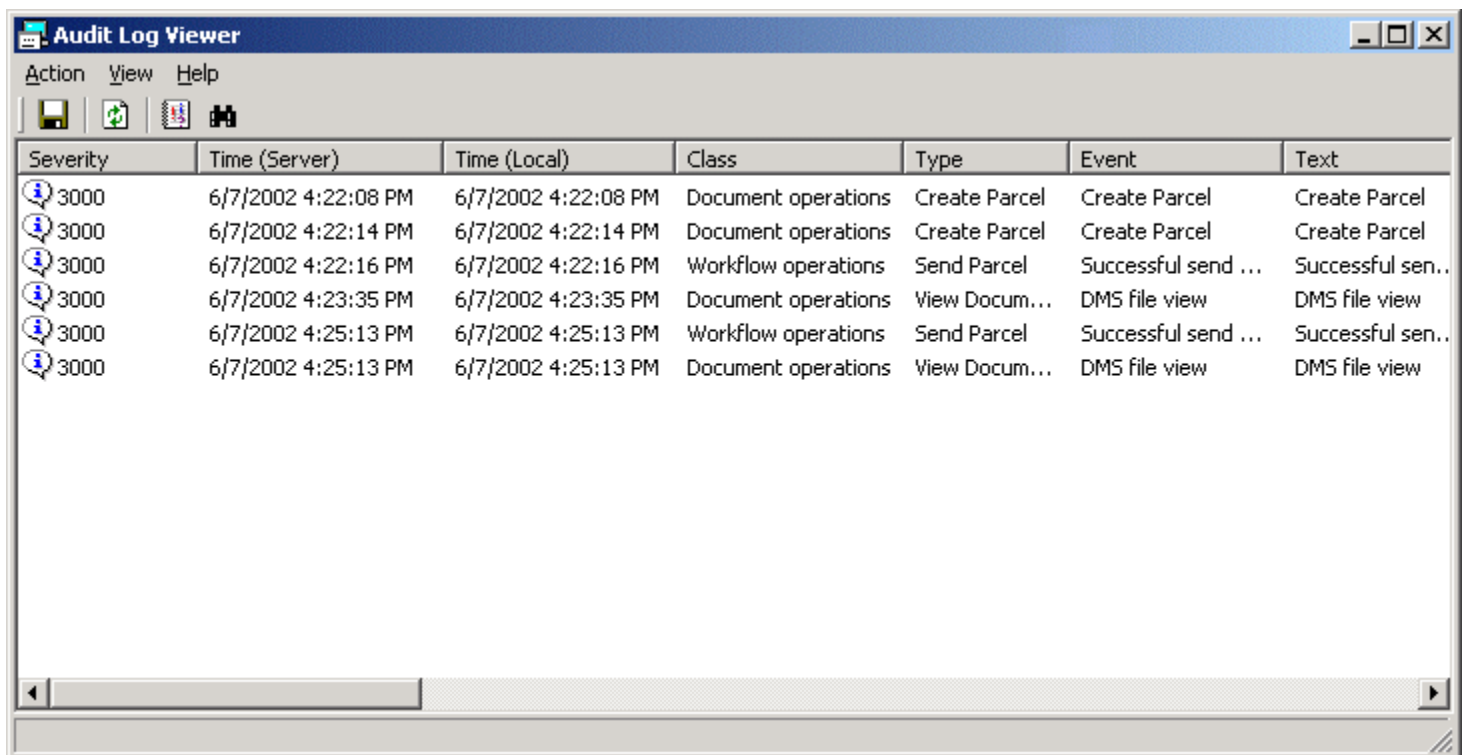


Figure 296: Audit Log Viewer window

The **Audit Log Viewer** window displays a list of audit log records, that is, events using the currently selected filter combination. The following tasks are available in this window:

- [Filtering Audit Records](#)
- [Customizing Columns and Column Filters](#)
- [Setting Column Filters](#)
- [Sorting Audit Records](#)
- [Searching Audit Records](#)
- [Exporting Audit Records](#)
- [Deleting Audit Records](#)

- [Refreshing Audit Records](#)
- [Copying Audit Records](#)
- [Archiving Audit Records](#)

Filtering Audit Records

To set audit records that are shown in the **Audit Viewer Log** window, click the **Filter** icon or select **View > Filter**.

The **Audit Filters** window appears.

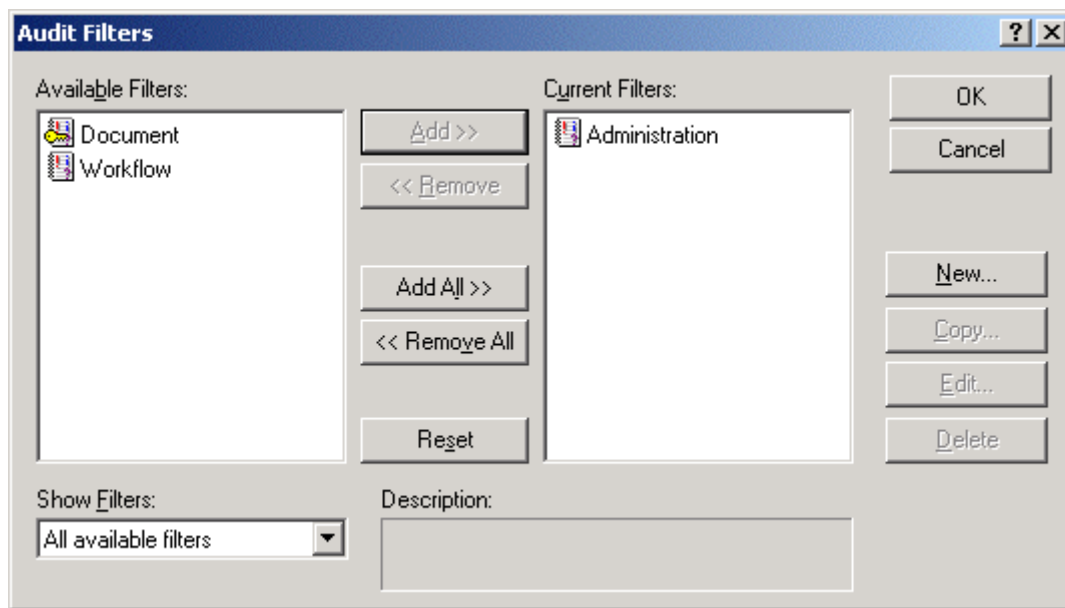


Figure 297: Audit Filters window

The following tasks are available in this window:

- [Activating Filters](#)
- [Deactivating Filters](#)
- [Resetting to Initial Current Filters](#)
- [Creating Filters](#)
- [Copying Filters](#)
- [Editing a Filter Definition](#)
- [Deleting Filters](#)

Activating Filters

To activate an available filter, select it in the available filters list and click **Add>>**. The filter appears in the current filter list. To activate all filters, click **Add All**.

Deactivating Filters

To deactivate a filter in the current list, select it in the list and click **<<Remove**. To deactivate all filters in the current list, click **Remove All**.

Resetting to Initial Current Filters

To cancel all changes and reset the initial list of current filters in the **Audit Filter** window, click **Reset**.

Creating Filters

The **Edit Audit Filter** window is used to specify audit data as follows:

- In the Administrator, the **Edit Audit Filter** window specifies audit records to be logged.
- In the Audit Log Viewer, the **Edit Audit Filter** window specifies audit records to be displayed.

The following filter types are available:

Filter types	
Type	Description
Including	Includes events that exactly match the values specified. An exception is the Severity field. Events having a severity less than or equal to the Severity field value are included.
Excluding	Excludes events that exactly match the specified values. An exception is the Severity field. Events having a severity less than or equal to the Severity field value are excluded.

To create an audit filter, proceed as follows:

1. Click **New**.

The **Edit Audit Filter** window appears with the **Properties** tab opened.

The 'Edit Audit Filter' dialog box is shown with the 'Properties' tab selected. It includes the following fields and controls:

- Name:** Text input field.
- Description:** Text input field.
- Public filter:** Check box.
- Excluding filter:** Check box.
- Event Class:** Dropdown menu (currently shows '<Any event class>').
- Event Type:** Dropdown menu (currently shows '<Any event type>').
- Event Message:** Dropdown menu (currently shows '<Any event message>').
- Severity:** Spin button.
- Event Phase:** Dropdown menu (currently shows '<Any event phase>').
- Transaction:** Text input field.
- Date and Time:**
 - From:** Date and time pickers (currently set to 6/7/2002 4:56:14 PM).
 - To:** Date and time pickers (currently set to 6/7/2002 4:56:14 PM).
 - Use server time:** Check box.
- Buttons:** 'OK' and 'Cancel' at the bottom right.

Figure 298: Edit Filter window

2. Use the **Properties** tab to specify the following general filter properties:
 - Enter a name that is unique and descriptive.
 - Enter a description.
 - To make the filter visible for all users, select the **Public** check box. Only users with Administrator access rights can modify it. If this check box is not selected, the filter is visible to the user who created it.
 - To create an excluding filter, select the **Excluding filter** check box. If the option is cleared, an including filter is used.
 - Select event class, type, message, and severity in the respective boxes.
 - The field **Transaction** is reserved for future use.
 - Specify the date and time of the first and last events.
 - To use time as it is on the database server, select the **Use server time** check box. If this is not selected, local computer time is used.
3. To specify advanced filter properties, select the **Advanced** tab.
4. To specify settings for the system, workflow, and project, enter appropriate values.
5. To save these settings, click **OK**.

Copying Filters

To create a filter based on an existing filter, proceed as follows:

1. Select a filter and click **Copy**.

The selected filter appears in the **Edit Filter** window.

2. Specify a name and change the corresponding settings.

Editing a Filter Definition

To change a filter definition, proceed as follows:

1. Select the filter definition and click **Edit**.

The filter appears in the **Edit Filter** window.

2. Change the settings as appropriate.

Deleting Filters

To delete a filter, select it and click **Delete**.

Customizing Columns and Column Filters

To set columns that are displayed in the **Audit Viewer Log** window, proceed as follows:

1. Select **View > Customize**.

The **Customize** window appears, showing hidden and visible columns.

The order in which the columns are arranged in the **Visible Columns** list corresponds to the column order displayed in Audit Viewer.

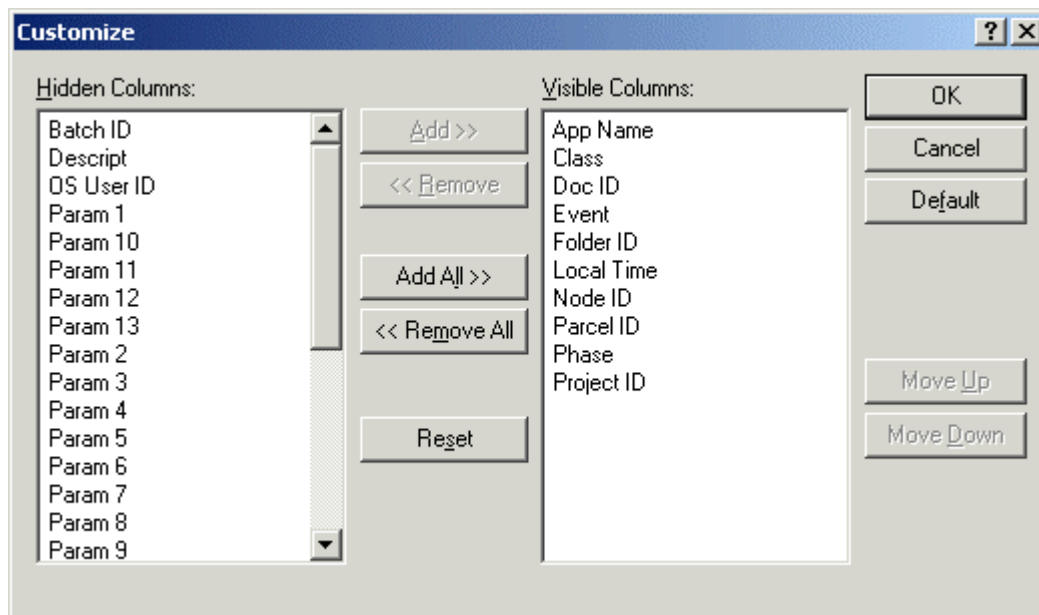


Figure 299: Customize window

2. To configure visible and hidden columns, in the **Customize** window, click the appropriate buttons as described in the following table:

Customize window buttons	
Button	Description
Add >>	Moves the selected column from the Hidden Columns list to the Visible Columns list.
<< Remove	Moves the selected column from the Visible Columns list to the Hidden Columns list.
Add All >>	Moves all columns from the Hidden Columns list to the Visible Columns list.
<< Remove All	Moves all columns from the Visible Columns list to the Hidden Columns list.
Reset	Restores the previous column configuration.
OK	Saves the column configuration and closes the Customize window.
Cancel	Closes the Customize window without changes.
Default	Restores the default column configuration.
Move Up	Moves the selected column up one row in the Visible Columns list.
Move Down	Moves the selected column down one row in the Visible Columns list.

Setting Column Filters

Column filters are convenient for dynamic audit data viewing.

To set a column filter, proceed as follows:

1. Right click the column and, in the pop-up menu, select **Filter by Column**.

The **Edit Column Filter** window appears. The fields that appear in this window depend on the column data.

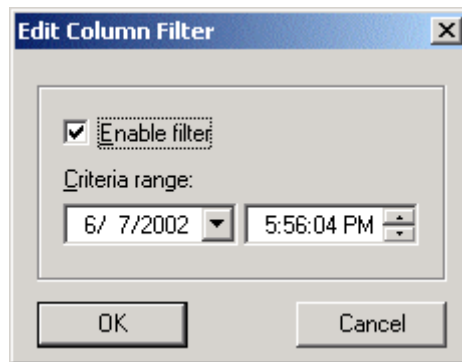


Figure 300: Edit Column Filter window

2. Enter the criteria range.
3. Select the **Enable filter** check box.
4. Click **OK**.

Sorting Audit Records

To sort audit data by a specific column, click the column or use **Select Sort Order** in the pop-up menu.

A green triangle appears on the column, and the sort order is reset.

The system allows you to sort by one to three columns.

Searching Audit Records

To search for the appropriate audit record, proceed as follows:

1. Select **View > Find**, or click the corresponding toolbar button.

The **Find Audit Event** dialog appears.

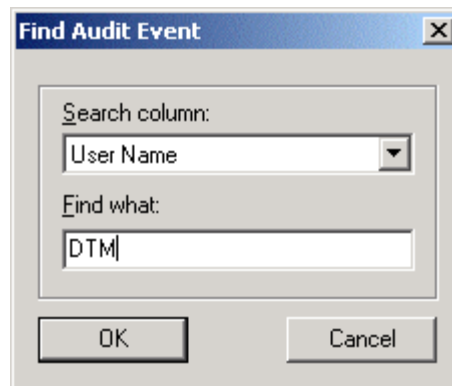


Figure 301: Find Audit Event window

2. Select the search column and enter the query in the respective field.
3. Click **OK**.

Exporting Audit Records

To export audit data to a file, proceed as follows:

1. Select **Actions > Export Audit To File**.

The **Save As** dialog appears.

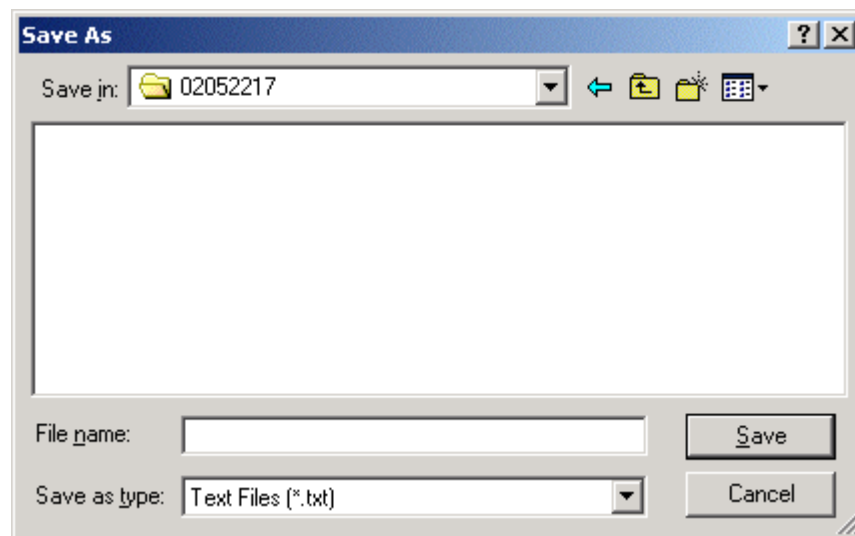


Figure 302: Save As dialog

2. Enter the appropriate file name and click **Save**.

Deleting Audit Records

The Delete Audit Events operation can be useful when your log is too large.

To delete audit records, proceed as follows:

1. Select **Actions > Delete Audit Events**.

The **Delete Audit Events** dialog appears.

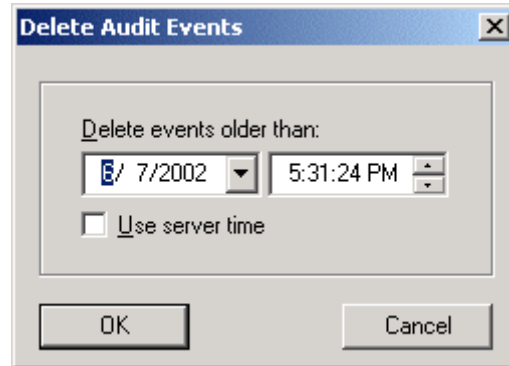


Figure 303: Delete Audit Events dialog

2. Select the appropriate date and time settings.
3. To use the time set on the database server, select the **Use server time** check box.

If the **Use server time** check box is not selected, local computer time is used.

Refreshing Audit Records

To see the latest changes in the audit log, perform any of the following steps:

- Select **View > Refresh**.
- Click the corresponding toolbar button.
- In the pop-up menu, select **Refresh**.

Copying Audit Records

To copy an audit record to the clipboard, right click it and select **Copy** in the pop-up menu.

Archiving Audit Records

To archive audit records, proceed as follows:

1. Set an audit archive filter as described in [Audit Archive Filter](#).
2. Initiate audit archiving using Activities Scheduler as described in [Scheduling Activities](#).

Audit Archive Filter

The audit archive filter defines the scope of audit records to be archived. The audit archive filter is inclusive; all records matching the indicated settings are archived.

To set the audit archive filter, proceed as follows:

1. In the Exigen Workflow Explorer, double click **Administrator**.
2. In the **Administrator Utilities** window, select **Administrator > Audit Archiving Filters**.

The **Archive Filters** window appears. The **Archive Filters** window is similar to the **Audit Filters** window as described in [Filtering Audit Records](#).

3. To create a filter, click **New**.

The **New Archive Filter** window appears.

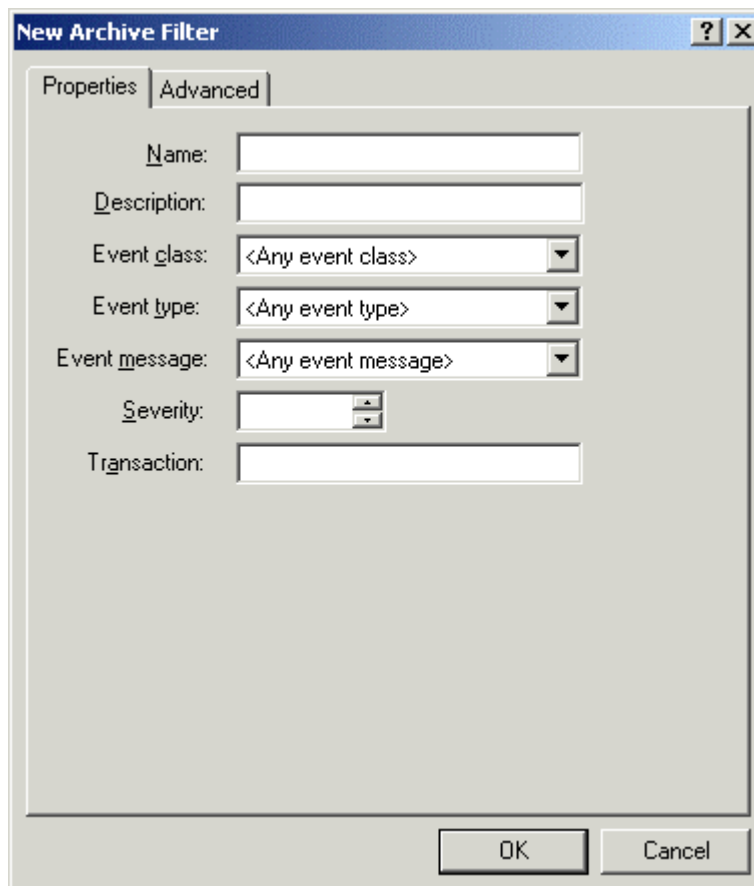


Figure 304: Creating an archive filter

4. To set filter properties, enter values in the **Properties** tab.

The following table describes the **Properties** tab options:

Properties tab	
Option	Description
Name	Filter name.
Description	Filter description. This is optional.
Event class	Event class. If no selection is made, all event classes are archived.
Event type	Event type. If no selection is made, all event types are archived.
Event message	Event message. If no selection is made, all event messages are archived.
Severity	Maximum severity level of archived records. Events having a severity level equal to or less than the specified severity level are archived as described in the following examples: <ul style="list-style-type: none"> • If the specified severity level is 1000, events having a severity level from 0 to 1000 are archived. This set includes standard and critical errors. • If the specified severity level is 4001, events having a severity level from 0 to 4001 are archived. This set includes standard and critical errors, warnings, standard information, and debug information. For information on event severity levels, see Event Audit Data . For information on inclusive filters, which are applied to audit archives, see Creating Filters .
Transaction	Field for future use.

5. To further define the scope of the filter, in the **Advanced** tab, enter appropriate values.

If no values are entered in a field, all audit records in the category are archived.

The following table describes the **Advanced** tab:

Advanced tab	
Option	Description
Application	Exigen Workflow application, such as Barcode Server.
User	Exigen Workflow user.
Domain user	Workstation user.
Workstation ID	Workstation ID.
Workflow ID	Workflow ID.
Node ID	Node ID.
Project ID	Project ID.
Document ID	Document ID.
Folder ID	Folder ID.
Parcel ID	Parcel ID.
Subfolder ID	Subfolder ID.
Batch ID	Batch ID.

6. Click **OK**.

The **Archive Filters** window appears.

7. In the **Archive Filters** window, perform the following tasks for filters as required:

- add
- remove
- reset
- copy
- edit
- delete

The **Archive Filters** window is similar to the **Audit Filters** window. For information on how to perform the preceding tasks, see [Filtering Audit Records](#).

8. Click **OK**.






Appendix A: Exigen Workflow Object Menus and Button Bars





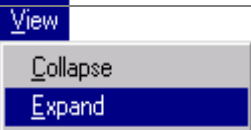





This section describes menu and button bars for the following components:

- [Exigen Workflow Explorer](#)
- [Project Builder](#)
- [Project Table Maintenance](#)

Exigen Workflow Explorer










The menu and button bars in Exigen Workflow Explorer contain the following utilities:





Exigen Workflow Explorer window button definitions			
Button	Menu option	Shortcut key	Description
	File > Open Application	F10	Open Application Opens the selected workflow object or utility.
	File > Workstation Setup	F3	Workstation Setup Sets up workstation specific attributes, including the assigning notification for new jobs received. Also used to set email notification flags.
	File > Login as a Different User	F4	Login as a Different User Allows the user to log in to another user desktop without closing and relaunching the Exigen Workflow system.
	File > Save Configuration		Save Configuration Saves the current Exigen Workflow Explorer configuration.
	View > Info pane		Info pane Displays the informational pane with the user name, date, and workstation number.
	View > Toolbar		Toolbar Displays the button bar.
	View > Status Bar		Status Bar Displays the status bar.
	View > Large Icons		Large Icons Displays workflow objects as large icons.

Exigen Workflow Explorer window button definitions			
Button	Menu option	Shortcut key	Description
	View > Small Icons		Small Icons Displays workflow objects as small icons.
	View > List		List Displays workflow objects in a list.
	View > Details		Details Lists workflow object names and details.
	View > Collapse		Collapse Folder Collapses all application folders in the left panel of the window.
	View > Expand		Expand Folder Expands all application folders in the left panel of the window.
	View > Calculate Jobs		Calculate Jobs Calculates the number of jobs in the selected workflow object. When selected, the display automatically changes to Details .
	View > Show Locked Documents		Displays window with a list of documents that are checked out for editing in the selected workflow node.
	View > Refresh	F5	Refresh Refreshes the Exigen Workflow Explorer application and updates the number of jobs in each queue.
	Help > Context Help	F1	Context Help Opens the Help section for this application.
	Help > Help Topics	CTRL+F1	Help Topics Displays a list of available help topics.
	File > Exit	F12	Exit the System Closes the Exigen Workflow Explorer application.

Project Builder






The menu and button bars in the **Project Builder** window contain the following utilities:



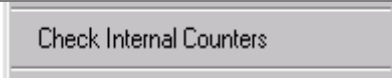


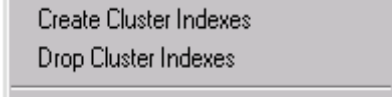
Project Builder window button definitions			
Button	Menu option	Shortcut key	Description
	Project > New	F6	New Project Allows creating a new project by defining a name and ID, and calculating database space.
	Project > Project Maintenance	F10	Project Maintenance Lists all tables assigned to the selected project for review and maintenance.
	Project > Project Configuration	CTRL+O	Project Configuration Assigns scan drives, required index fields, QA parameters, and optical storage attributes.
	Project > Copy	CTRL+C	Copy Copies the selected project to another project name, project ID, and database.
	Project > Modify	CTRL+R	Modify Changes the project name only.
	Project > Delete	F8	Delete Deletes the selected project from the system.
	Project > Save Configuration		Save Configuration Saves the size and position of the current window for the next time when the window is opened.
	Project > Import Project > Tables or Data		Import Project Used to import project tables and data from other Exigen Workflow systems.
	Project > Export Project > Tables or Data		Export Project Used to create export files containing the tables and data for the selected project.
	Project > Create FTS Tables		Create FTS Tables Used to create the Full Text Search structure in the project enabling Retrieve users to search for documents based on the text contained therein.
	Project > Drop FTS		Drop FTS Drops the Full Text Search structure in the project, disabling the ability to retrieve documents based on the text contained therein.




Project Builder window button definitions			
Button	Menu option	Shortcut key	Description
	Project > Check Project Version		Check Project Version Compares the existing database structures with any new Exigen Workflow releases installed and allows you to correct any discrepancies.
	Project > Print Report	CTRL+P	Print Report Prints a detailed listing of the project attributes and tables.
	Help > Context Help	F1	Context Help Opens the Help section for this application.
	Help > Help Topics	CTRL+F1	Help Topics Displays a list of available help topics.
	File > Exit	F12	Exit Project Builder Closes the Project Builder tool.

Project Table Maintenance

The menu and button bars in the **Project Table Maintenance** window contain the following utilities:

Project Table Maintenance window button definitions			
Button	Menu option	Shortcut key	Description
	Maintenance > New Table	F4	New Table Creates a new table. The table name and one field name, type, and length must be specified.
	Maintenance > New Field	F2	Add New Field Creates a new field in the selected table.
	Maintenance > Modify Field	F3	Modify Field Allows you to change certain attributes in the selected field.
	Maintenance > Delete Field	F8	Delete Field Deletes the selected field if the database used supports this function.
	Maintenance > Move Field UP	CTRL+U	Move Field Up Moves the selected field up one row in the list.

Project Table Maintenance window button definitions			
Button	Menu option	Shortcut key	Description
	Maintenance > Move Field DOWN	CTRL+D	Move Field Down Moves the selected field down one row in the list.
	Maintenance > Manage Views		Manage Views Used in Project Allows you to add, edit, and delete views, and to set conditions for them.
	Maintenance > Check Internal Counters		Check Internal Counters Shows the maximum counter values for folder, document, archive, and parcel and batch numbers in the project.
	Maintenance > Create Unique Index		Create Unique Index Creates a unique index in the selected table using a combination of all fields identified as being part of the unique index.
	Maintenance > Drop Unique Index		Drop Unique Index Drops the unique index set up in the selected table using the fields designated as a part of the unique index.
	Maintenance > Create Cluster Indexes		Create Cluster Indexes Creates cluster indexes in the database if the scanning and indexing portion is separate from the main workflow.
	Maintenance > Drop Cluster Indexes		Drop Cluster Indexes Drops cluster indexes from the database.
	Maintenance > Recreate Project Indexes		Recreate Project Indexes Recreates all project indexes for all project tables.
	Maintenance > Create FTS Tables		Create FTS Tables Used to create the Full Text Search structure in the project enabling Retrieve users to search for documents based on the text contained therein.
	Maintenance > Drop FTS		Drop FTS Drops the Full Text Search structure in the project, disabling the possibility to retrieve documents based on text contained therein.

Project Table Maintenance window button definitions			
Button	Menu option	Shortcut key	Description
	Maintenance > Print Report	CTRL+P	Print Report Prints a detailed listing of each table in the project.
	Maintenance > Exit	F12	Exit Project Maintenance Closes the Project Table Maintenance tool.
	Edit > Copy Table	CTRL+C	Copy Table Copies the contents of the table to the clipboard.
	Help > Context Help	F1	Context Help Opens the Help section for this application.
	Help > Help Topics	CTRL+F1	Help Topics Displays a list of available Help topics.
	Help > About Exigen Workflow		About Exigen Workflow Displays information on the Exigen Workflow version and the workstation ID.

Appendix B: Default Tables for New Exigen Workflow Projects

When a project is created, the following default tables are created in the database:

Default project tables	
Name	Description
BARCOLUMN	Contains the list of tables and columns that is used for barcode data. The data is taken from the Barcode Setup window in the Barcode Server object.
BARSETUP	Contains the descriptions of each of the configuration setups in Barcode Server and the actions the system is set up to take once each bar code is read. The data is taken from the Barcode Setup window in the Barcode Server object.
BATCHPARCEL	Contains information about batches and parcels created in the system including the identification of the queue and the user to whom the parcel is assigned. Records are added each time a new batch or parcel is created.
COMMIT_CONFIG	Contains information regarding the cache and platter configuration of the optical disk servers where the images are stored. The data is taken from the Optical Configuration utility in the Administrator application.
COMMIT_SERVERS	Contains information about the database, including cache configuration and password, where the information on the committed images is stored. The data is taken from the Image Server Setup utility in the Administrator application.
DOCUMENT	Contains information about each document scanned or created in the system including the assigned folder, subfolder, parcel, queue, and user. Records are added each time a new document is created.
DOCTYPE	Contains values used to identify each document. Initially this table is empty. Document types and descriptions can be added via the Table Maintenance tool in the Administrator application. These values allow documents to be easily identified. During indexing, these values are available for assignment to each record.
EDMCOLUMN	Contains ERM setup information pertaining to the columns that are filled by the incoming electronic data. Records are added via the ERM Setup object.
EDMOVERLAY	Contains ERM setup information pertaining to Form Overlay processing. Records are added via the ERM Setup object.
EDMSETUP	Contains ERM setup information pertaining to the workflow, node, and user where the incoming electronic data is routed. Records are added via the ERM Setup object.
EDMTABLES	Contains ERM setup information pertaining to the tables that are populated by incoming electronic data. Records are added via the ERM Setup object.
ENHSETUP	Contains the automatic enhancement settings in the project. The data comes from the values assigned in Enhancement Server.
ESCALATION_LOG	Contains details of the records processed through Escalation Server. The data appears once the server is run.

Default project tables	
Name	Description
EVENT	Contains information for all events pending or already processed. Records are added when the event is triggered.
EXPSETUP	Contains the export attributes and settings assigned in Export Server.
EXPLEGEND	Contains the document numbers of the exported files, the project ID and the date they were exported.
FOLDER	Contains a list of all folders that exist in the project. Folders are added during the indexing phase using index fields created on this table.
FORMCOLUMN	Contains a list of all tables and their respective fields where the information is populated by a specific non-Exigen Workflow file.
FORMSETUP	Contains a list and properties of all types of input files that can be used to populate database fields with information.
FORMTABLES	Contains a list of all tables that store data extracted from form files.
PRJSETUP	Contains information regarding the respective project including settings entered during project creation and modification. The table is updated when a project is added or modified.
SUBFOLDER	Contains a list of all the subfolders added to the project either through Table Maintenance or during subfolder indexing.
SYSCOLUMNS	Contains a list of all the fields of all the project tables and their properties.
SYSINDEXES	Contains a list of all project tables and the indexes assigned to each. There can be more than one.
SYSKEYS	Lists all the indexes and their assigned project fields. A field can be assigned to more than one index.
SYSTABLES	Contains a list of all project tables and their properties.
TASKHISTORY	Contains a list of all tasks performed in the project that had the "create task history" box selected during task creation. Records are added each time applicable tasks are executed and are listed by folder and document number.
VIEW_CONDITIONS	Contains view conditions for all views created in project.
VIEWS	Contains a list of views created in the project and their properties.
USER_COMPL	Contains user comments regarding certain folders and documents. This information can be viewed with the Workflow Monitor utility.
ZONECOLUMN	Contains a list of tables and columns that are used for form OCR recognition. The data comes from the settings in Form OCR Server.
ZONESETUP	Contains the zone configuration used for form OCR recognition. The data comes from the settings in Form OCR Server.

Appendix C: Using .ini Files for Internationalization and Path Substitution

The following topics are described in this section:

- [Configuring Internationalization](#)
- [Path Substitution](#)

Configuring Internationalization

Exigen Workflow is an internationalized product that can be implemented in different language environments. To support internationalization, the system administrator must specify the appropriate settings in the Exigen Workflow .ini files. The `visi.ini` file in the Exigen Workflow directory and the `visiclt.ini` file in the Windows directory include several sections for internationalizing dates.

The following topics are described in this section:

- [Formatting Dates and Times in the visiclt.ini File](#)
- [Entering Database Server Names in the visi.ini File](#)
- [visi.ini File Database Server Section Examples](#)

Formatting Dates and Times in the visiclt.ini File

In the `visiclt.ini` file, the NLV section contains constants for `DisplayFormat`. **DisplayFormat** determines the format of dates and times displayed in application forms, or dialogs, that depend on settings in the profile, or on regional settings selected by a user.

The following table displays keys for date formats set in the NLV section of the `visiclt.ini` file:

Keys for date formats in the visiclt.ini file, NLV section	
Key	Description
sFmtDate	Date format.
sFmtDateShort	Short date format.
sFmtTime	Time format.
sFmtTimeShort	Short time format.
sFmtDateTime	Date/time format.
sFmtDateTimeShort	Short date/time format.
sFmtDateTimeFull	Long (full) date/time format.
sDateNull	Date for appending time to full date/time.
sAMString	AM character.
sPMString	PM character.
sDateSeparator	Date separator.
fmt_c_date	Date format in Windows format in C language code.
fmt_c_time	Time format in Windows format in C language code.
sFmtDateTimeFull_A	Reserved for future use.

Note: If no NVL section exists, the default system settings are used.

The following values are appropriate:

Centura date/time formats		
Format	Description	Value
M	month	1-12.
MM	month	01-12.
d	day	1-31.
dd	day	01-31.
yy	year	00-99.
yyyy	year	0000-9999.
hh	hour	1-12.
hhhh	hour	0-24
mm	minutes	0-59.
ss	seconds	0-59.
mmmmmm	microseconds	000000-999999.
AMPM	AM/PM	AM/PM indicator.

For `fmt_c_date` and `fmt_c_time` the following values are appropriate:

C language formats	
Symbol	Description
h	Hours with no leading zero for single digit hours, 12 hour clock.

hh	Hours with leading zero for single digit hours, 12 hour clock.
H	Hours with no leading zero for single digit hours, 24 hour clock.
HH	Hours with leading zero for single digit hours, 24 hour clock.
m	Minutes with no leading zero for single digit minutes.
mm	Minutes with leading zero for single digit minutes.
s	Seconds with no leading zero for single digit seconds.
ss	Seconds with leading zero for single digit seconds.
tt	Multi-character time marker string, such as AM or PM.
d	Day of month as digits with no leading zero for single digit days.
dd	Day of month as digits with leading zero for single digit days.
M	Month as digits with no leading zero for single digit months.
MM	Month as digits with leading zero for single digit months.
y	Year as last two digits, but with no leading zero for years less than 10.
yy	Year as last two digits, but with a leading zero for years less than 10.
yyy	Year represented by four digits.

Entering Database Server Names in the visi.ini File

Database server names are listed in the `visi.ini` file, as in the following example:

Oracle: [ORACLE]

The following table lists keys in database server sections in the `visi.ini` file:

Keys in the visi.ini file, database server sections	
Key	Description
sNumberToCharBeg	Prefix for converting numbers to chars.
sNumberToCharEnd	Suffix for converting numbers to chars.
sFloatToCharBeg	Prefix for converting floats to chars.
sFloatToCharEnd	Suffix for converting floats to chars.
sDateToCharBeg	Prefix for converting dates to chars.
sDateToCharEnd	Suffix for converting dates to chars.
sTimeToCharBeg	Prefix for converting time to chars.
sTimeToCharEnd	Suffix for converting time to chars.
sDateTimeToCharBeg	Prefix for converting date/time to chars.
sDateTimeToCharEnd	Suffix for converting date/time to chars.
sDateTimeToCharEndEx	Suffix for converting date/time to chars.
sCharToDateBeg	Prefix for converting chars to dates.
sCharToDateEnd	Suffix for converting chars to dates.
sWriteDateFormat	ToServerFormat of date.
nWriteDateChars	Date precision, that is, number of chars to truncate.
sCharToTimeBeg	Prefix for converting chars to date/time.
sCharToTimeEnd	Suffix for converting chars to date/time.
sWriteDateTimeFormat	ToServerFormat of date/time.
nWriteDateTimeChars	Precision of date/time, that is, number of chars to truncate.
sReadDateTimeFormat	FromServerFormat of date/time.
sReadDateFormat	FromServerFormat of date.
sDateNull	Date for appending time to full date/time.

visi.ini File Database Server Section Examples

This section includes visi.ini file database server examples.

```
[NLV]
sFmtDate="yyyy/dd/MM"
sFmtDateShort="yyyy/dd/MM"
sFmtTime="hhhh:mm:ss"
sFmtTimeShort="hhhh:mm"
sFmtDateTime="yyyy/dd/MM hhhh:mm:ss"
sFmtDateTimeShort="yyyy/dd/MM hhhh:mm"
sFmtDateTimeFull="yyyy/dd/MM hhhh:mm:ss.mmmmmm"
sDateNull="1899/01/01"
sAMString="AM"
sPMString="PM"
sDateSeparator="/"
sFmtDateTimeFull_A=yyyy-MM-dd hh:mm:ss.mmmmmm AMPM
fmt_c_date = "yyyy/dd/MM"
fmt_c_time = "HH:mm:ss"
```



```
[ORACLE]
sNumberToCharBeg=" TO_CHAR ( "
sNumberToCharEnd=" )"
sFloatToCharBeg=" TO_CHAR ( "
sFloatToCharEnd=" )"
sDateToCharBeg=" TO_CHAR ( "
sDateToCharEnd=", 'YYYY-MM-DD HH24:MI:SS' )"
sTimeToCharBeg=" TO_CHAR ( "
sTimeToCharEnd=", 'HH:MI:SS AM' )"
sDateTimeToCharBeg=" TO_CHAR ( "
sDateTimeToCharEnd=", 'YYYY-MM-DD HH24:MI:SS' )"
sDateTimeToCharEndEx=", 'YYYY-MM-DD HH24:MI:SS' )"
sCharToDateBeg=" TO_DATE ( ' "
sCharToDateEnd=", 'YYYY-MM-DD HH24:MI:SS' )"
sCharToTimeBeg=" TO_DATE ( ' "
sCharToTimeEnd=", 'YYYY-MM-DD HH24:MI:SS' )"
sWriteDateTimeFormat="yyyy-MM-dd hhhh:mm:ss"
nWriteDateTimeChars="0"
sWriteDateFormat="yyyy-MM-dd hhhh:mm:ss"
nWriteDateChars="0"
sReadDateTimeFormat="yyyy-MM-dd hhhh:mm:ss"
sReadDateFormat="yyyy-MM-dd hhhh:mm:ss"
sDateNull="1899-01-01"
```

```
[ODBC]
sNumberToCharBeg=" CONVERT (VARCHAR (64), "
sNumberToCharEnd=" )"
sFloatToCharBeg=" STR ( "
sFloatToCharEnd=", 16, 2)"
sDateToCharBeg=" CONVERT (VARCHAR, "
sDateToCharEnd=", 100)"
sTimeToCharBeg=" CONVERT (VARCHAR, "
sTimeToCharEnd=", 108)"
sDateTimeToCharBeg=" CONVERT (VARCHAR, "
sDateTimeToCharEnd=", 113)"
sDateTimeToCharEndEx=", 109)"
sCharToDateBeg=" CONVERT (DATETIME, ' "
sCharToDateEnd=" ')"
sCharToTimeBeg=" CONVERT (DATETIME, ' "
sCharToTimeEnd=" ')"
sWriteDateTimeFormat="MM-dd-yyyy hh:mm:ssAMPM"
nWriteDateTimeChars="0"
sWriteDateFormat="MM-dd-yyyy hh:mm:ssAMPM"
nWriteDateChars="0"
sReadDateTimeFormat="MM-dd-yyyy hhhh:mm:ss"
sReadDateFormat="MM-dd-yyyy"
sDateNull="01-01-1899"
```

```
[SQL]
sNumberToCharBeg=" @STRING ( "
sNumberToCharEnd=", 0)"
sFloatToCharBeg=" @STRING ( "
sFloatToCharEnd=", 3)"
sDateToCharBeg=" @DATETOCHAR ( "
sDateToCharEnd=", 'mm-dd-yyyy' )"
sTimeToCharBeg=" @DATETOCHAR ( "
```

```

sTimeToCharEnd=", 'HH:MI:SS AM')"
sDateTimeToCharBeg=" @DATETOCHAR ("
sDateTimeToCharEnd=", 'mm-dd-yyyy HH:MI:SS AM')"
sDateTimeToCharEndEx=", 'mm-dd-yyyy HH:MI:SS AM')"
sCharToDateBeg=" '"
sCharToDateEnd=" '"
sCharToTimeBeg=" '"
sCharToTimeEnd=" '"
sWriteDateTimeFormat="yyyy-MM-dd-hhhh.mm.ss.mmmmmm"
nWriteDateTimeChars="0"
sWriteDateFormat="yyyy-MM-dd-hhhh.mm.ss.mmmmmm"
nWriteDateChars="0"
sReadDateTimeFormat="MM-dd-yyyy hhhh.mm.ss.mmmmmm"
sReadDateFormat="MM-dd-yyyy"
sDateNull="01-01-1899"

```

Path Substitution

The following topics are described in this section:

- [Overview](#)
- [Enabling Path Substitution](#)
- [Example](#)

Overview

When scripts, documents, or stamps are deployed to a new environment, their location may not be valid in respect to the new environment. To solve this problem, the path substitution method can be used. Path substitution is part of Exigen Workflow functionality.

Note: Not all references in Exigen Workflow support this feature.

Functions that support path substitution are the following:

- document templates
- agent script definitions supported by Component Configuration Manager
- OCR templates supported by the Template Management utility and Form OCR Server
- path to document caches supported by storage devices
- path to stamps supported by stamp templates

Sometimes path substitution is used as part of the solution, that is, it is planned when building solutions. For example, when design-time and run-time environments have different drive mapping, path substitution can be used so that the design-time server and the run-time server have different references to the same file storage.

Multiple substitutions can be defined in the [Substitute] section. However, recursive substitutions are not allowed.

Enabling Path Substitution

To enable path substitution, proceed as follows:

1. Open or create a new `remote.ini` file in one of the following locations, depending on the client used:

remote.ini file location	
Client	Location
Windows based client	Exigen Workflow <code>SYSTEM</code> directory.
Web client in remote document access mode	Exigen Workflow Web server <code>WEB-INF\Dll</code> directory.
Web client in local document access mode	Directory where the Web DMS Viewer is installed.

2. Modify the `remote.ini` file as follows:

```
..
```

```
[Substitute]
```

```
<location to be substituted>=<new location>
```

3. Save and close the `remote.ini` file.
4. If the Windows based client is used, restart the application.
5. If the web client is used, restart the web application server.

Example

If the Exigen Interaction Script Builder script task is configured to have the configuration file name with the full path, for example, `\\testsrv1\checklist\tasks.txt`, but after deployment, this file is stored in `\\scriptsrv\public`, the substitution line in the `remote.ini` file must be modified as follows:

```
\\testsrv1\checklist=\\scriptsrv\public
```

Appendix D: Audit Data in Exigen Workflow

Audit data is a historical record of the process instance, from start to completion or termination. Such data normally incorporates information on the state of the transition of the process instance.

Audit functionality in Exigen Workflow is based on the concept of auditable events. Each operation can generate one or more auditable events, which can be logged. Examples of such events include user login to the system, a send parcel operation, or document viewing.

Implementation of the Exigen Workflow audit functionality provides an open framework that can be used by all applications cooperatively participating in the operation of a particular Exigen Workflow implementation. There are other special provisions that enable working with audit data without prior detailed knowledge of the contents.

Exigen Workflow stores audit data in the database table PROJECT ID_AUDIT_LOG. This table, together with other reference tables, must be used to interpret and represent audit information.

Note that audit data is produced by Exigen Workflow and other applications. However, it is not produced automatically by the workflow data store and other information stores. Therefore, it is the responsibility of the application to provide correct audit data.

The following topics are included in this section:

- [Exigen Workflow Audit Log Data](#)
- [Audit Configuration](#)
- [Audit Server](#)

Exigen Workflow Audit Log Data

The following topics are included in this section:

- [Audit Log Data Groups](#)
- [PROJECT ID_AUDIT_LOG Table](#)

Audit Log Data Groups

Audit log record data produced by Exigen Workflow applications can be logically separated into the following groups:

Audit log record data groups	
Group	Description
Application	Information regarding the application that caused the event.
Event	Generalized description of the event, which can be used to filter audit data and compile reports.
Event data	Event-specific data that can be used only by the application that is aware of the nature of

Audit log record data groups	
Group	Description
	the event.
Context	Global configuration and operational parameters in effect at the time the event is executed.

Application Audit Data

This data group describes an application that invokes the operation that is causing the event. The application is fully described by its name and user account under which it operates.

Event Audit Data

The event class and type characterize events. The event class defines a broad group of events related to the same class of activities, such as security, workflow operations, and document operations. The event type provides a detailed identification of the event. Types are unique within the class.

The separation of event classes and types enables the system administrator to configure filtering or set up reactions to events without knowledge of all event types in the system.

For each event the following information is provided:

Event audit data	
Name	Description
Server side timestamp	Database server date and time when the event occurred.
Client side timestamp	Client side date and time when the event occurred.
Severity	Severity level of the event. Exigen Workflow defines the following severity levels: <ul style="list-style-type: none"> • Debug: information regarding program execution used for debugging or troubleshooting purposes. • Information: information regarding normal completion of operations or operation progress; no abnormalities detected. • Warning: an abnormality was detected while executing an operation. It was either corrected automatically or does not affect the operation. • Error: an abnormality was detected while executing an operation causing the operation to fail. The failure affects the single operation. Operation of the application and entire system remain unaffected. • Critical: an abnormality was detected while executing an operation causing the operation to fail. The failure affects the operation of the application and entire system.
Transaction	Transaction of which the operation is a part. This event attribute enables the grouping of events by transaction.
Phase	Logically tied events. This allows events to be logged “before” and “after” some long or important action. Phase 1 indicates that an event is the start of a logical action and phase 2 indicates that an event is the end of a logical action. If an application fails after an event marked with phase 1, there is no corresponding event marked with phase 2. The administrator is able to check audit logs by searching for events marked with phase 1 without the corresponding events marked with phase 2 for the specified user, workstation and session. Events that are solid and are not tied to other events are phase 0.

Implementation of the audit in Exigen Workflow allows applications to use custom severity levels. Custom severity levels must fit into the overall severity level schema in order for management applications to function properly. This is achieved by reserving ranges for each severity level as follows:

Predefined event severity levels	
EVNT_SLID	Event severity
0-999	Critical error.
1000-1999	Error.
2000-2999	Warning.
3000-3999	Information.
>4000	Debug information.

Event Data

Event data provides event specific information, which is stored in additional parameters. Interpretation of this data requires an application aware of these event specific contents. The contents are fully described by event class, type and message.

Context Data

Context audit log data describes an environment where the operation causing the event is executed. The following parameters are identified:

Context audit log data	
Name	Description
Workflow	Workflow identification.
Project	Project identification.
Node	Node identification from which the operation is invoked.
Parcel	Parcel identification.
Document	Document identification.
Folder	Folder identification 999999999 stands for "not assigned."
Subfolder	Subfolder identification 999999999 stands for "not assigned."
User	User invoking the operation causing the event. This is not necessarily the same user that is operating the application.
Tenant	Tenant identification.
Session	Session identification.

PROJECT ID_AUDIT_LOG Table

The following table describes the PROJECT ID_AUDIT_LOG table, where audit data is written:

Project ID_AUDIT_LOG table		
Name	Type	Description
EVNT_TIMESTAMP_SRV	DATETIME	Database server date and time when the event occurred.

Project ID_AUDIT_LOG table		
Name	Type	Description
EVNT_TIMESTAMPLOC	DATETIME	Client date and time when the event occurred.
EVNT_CLID	INT	Event class ID, reference to the event class name in the PROJECT ID_AUDIT_MSGID table.
EVNT_TPID	INT	Event type ID, reference to the event type in the PROJECT ID_AUDIT_MSGID table.
EVNT_SLID	INT	Severity level of the event. For information on severity levels, see Event Audit Data .
EVNT_MSGID	INT	Event message ID, reference to the event class name in the PROJECT ID_AUDIT_MSGID table.
EVNT_FMTID	INT	Formatted text message ID for the specified event, reference to the PROJECT ID_AUDIT_MSGID table.
EVNT_PHASE	INT	Event phase.
EVNT_TRID	VARCHAR[50]	ID of the transaction this event is part of.
CNXT_WFID	INT	Workflow ID.
CNXT_PRID	VARCHAR[3]	Project ID.
CNXT_NDID	INT	Node ID.
CNXT_WIID	INT	Parcel ID.
CNXT_DOC	INT	Document ID.
CNXT_FOLDER	INT	Folder ID.
CNXT_SUBFOLDER	INT	Subfolder ID.
CNXT_UUID	VARCHAR[32]	User ID invoking the operation causing the event.
CNXT_TNID	VARCHAR[50]	Tenant ID of the user.
CNXT_USID	INT	User session ID.
CNXT_WSTID	INT	User Exigen Workflow workstation ID.
CNXT_TRNID	INT	Transaction ID if the audit event is part of the transaction.
CNXT_BAT_ID	INT	Document batch number.
CNXT_APP	VARCHAR[50]	Application name.
CNXT_OS_USER	VARCHAR[50]	Domain and name of the OS user in the format domain\name.
CNXT_SEQUENCE	INT	Sequence number in the transaction.
CNXT_PARAM1	VARCHAR[254]	Additional field for parameter.
CNXT_PARAM2	VARCHAR[254]	Additional field for parameter.
CNXT_PARAM3	VARCHAR[50]	Additional field for parameter.
CNXT_PARAM4	VARCHAR[10]	Additional field for parameter.
CNXT_PARAM5	INT	Additional field for parameter.
CNXT_PARAM6	FLOAT	Additional field for parameter.
CNXT_PARAM7	FLOAT	Additional field for parameter.
CNXT_PARAM8	DATETIME	Additional field for parameter.
CNXT_PARAM9	DATETIME	Additional field for parameter.

Project ID_AUDIT_LOG table		
Name	Type	Description
CNXT_PARAM10	INT	Additional field for parameter.
CNXT_PARAM11	INT	Additional field for parameter.
CNXT_PARAM12	INT	Additional field for parameter.
CNXT_PARAM13	INT	Additional field for parameter.

Audit Configuration

Audit configuration is set up using the S23_AUDIT_FILTER database table. This configuration is read into memory at the application startup and continuously refreshed on any audit operation if a defined interval has passed since the last refresh. The default value is 10 seconds.

The amount of time between filter refresh operations can be configured in the [AUDIT_LOG] section of the `visi.ini` file by modifying the `FILTER_REFRESH` value. If this value is set to 0, filter refreshing is disabled, as described in [Sample Audit Configuration](#).

When a new audit project is created, the system shows the following warning: "No active audit filters found. Are you sure you want to enable the default filter." If you answer **Yes**, default audit filters are created, and the S23_AUDIT_FILTER table is filled with default values. By default, all events with `critical error` or `error` severity level are logged. It is recommended that you change the default filters by selecting **Administrator > Audit Filters** in the **Administrator Utilities** window.

When configuring an audit, the following points must be considered:

- Audit filter record data is specified in the S23_AUDIT_FILTER table as described in [S23_AUDIT_FILTER Table](#).
- To enable auditing, at least one including filter record must be present with empty values.
- Including filters are evaluated prior to excluding filters.
- If an event matches the criteria, all existing excluding filters are evaluated.

The following topics are included in this section:

- [Audit Algorithm](#)
- [Local Audits](#)
- [Sample Audit Configuration](#)
- [PROJECT ID_AUDIT_MSGID Table](#)
- [S23_AUDIT_FILTER Table](#)
- [Audit Event Descriptions](#)

Audit Algorithm

Exigen Workflow uses the following algorithm to decide if an audit event must be stored in the audit log:

1. The system checks if any including filters matching the audit record exist. To compare the audit record with the audit filter, all non-NULL fields of the filter are compared with corresponding fields in the audit record. If such a filter is found, the audit record is considered a candidate for storage in the audit log as described in step 2; otherwise, the audit record is not stored.
2. The system checks if any excluding filters matching the audit record exist. Only non-NULL fields are considered. If such an excluding filter is found, the audit record is not stored in the audit log; otherwise, the record is written to the audit log.

For example, to include all possible records in the audit log, you must insert a filter with all NULL fields. This filter matches any audit record and as a result, the most detailed, but also the most storage-consuming audit log is collected.

The audit record is logged only if the event does not match any of the excluding filters as described in [PROJECT ID AUDIT LOG Table](#).

As an option, for example, a local audit can be switched on for any Exigen Workflow workstation. The result of such an audit is redirected to a local file. The redirection can be configured in the `visiclt.ini` file. For more information on local audits, see [Local Audits](#).

Local Audits

A local audit works as a supplementary audit to the system-wide Exigen Workflow audit. It does not override the settings of the system-wide Exigen Workflow audit. The file the local audit is redirected to can be used as a local storage for audit data; the database is unavailable.

The following topics are included in this section:

- [Local Audit Configuration](#)
- [Local Audit Configuration Example](#)
- [Local Audit Restrictions](#)

Local Audit Configuration

A local audit, for example, a workstation-dependent audit, is configured by editing the `visiclt.ini` file. The `[AUDIT_LOG]` section in the `visiclt.ini` file must contain the key `LOG_PATH`, whose value must contain the path to the local audit file. Filters for such auditing are set in the `[AUDIT_LOG_FILTERS]` section using the key `LOG_FILTER`. The filter key values for the local audit must be string representations of the filter record with the same structure as in the `S23_AUDIT_FILTER` table. The same configuration as for the `S23_AUDIT_FILTER` table can be used to set up filters in the `visiclt.ini` file.

Schema:

```
[AUDIT_LOG]
LOG_PATH="<path and file name>"
[AUDIT_LOG_FILTERS]
LOG_FILTER="<EVNT_CLID>;<EVNT_TPID>;<EVNT_SLID>;
<EVNT_MSGID>;<EVNT_FMTID>;<EVNT_TRID>;
<CNXT_WFID>;<CNXT_PRID>;<CNXT_NDID>;<CNXT_WIID>;<CNXT_BAT_ID>;"
```

```
<CNXT_DOC>;<CNXT_FOLDER>;
<CNXT_SUBFOLDER>;<CNXT_UUID>;<CNXT_TNID>;<CNXT_USID>;<CNXT_WSTID>;
<CNXT_APP>;<CNXT_OS_USER>;< EVNT_FILTER_TYPE>;<EVNT_FILTER_STATE>"
```

If the audit database is not available, the audit information is stored in a local audit file. The full path, including file name, can be defined in the `visiclt.ini` file.

Local Audit Configuration Example

```
[AUDIT_LOG]
```

```
LOG_PATH="c:\test.log"
```

If the location of the local audit file is not specified in the `visiclt.ini` file, the audit system writes the log to the file `$TEMP$\EVF_AUDIT.LOG` or `TMP\EVF_AUDIT.LOG`.

The `visi.ini` file specifies the delay for restoring a connection. If the connection is lost and reconnection is not successful, the audit system places audit records into a text file locally until the specified interval has passed. At that point, the reconnection procedure is invoked again. The following is an example of audit configuration in the `visi.ini` file:

```
[AUDITLOG]
```

```
RECONNECT=30 ; minutes
```

If the `RECONNECT` value is not defined, the reconnect delay is set to 10 minutes.

Local Audit Restrictions

The following restrictions apply to local audits:

- Audit Server cannot be used for local audit data.
- Audit Viewer cannot be used to view local audit data.
- The audit filters configuration feature in Exigen Workflow Administrator cannot be used to configure local audits. For information on configuring local audits, see [Local Audit Configuration](#).
- The audit archiving filter in Exigen Workflow Administrator cannot be used for local audit data.
- Local auditing is available only for Exigen Workflow client/server components.

Sample Audit Configuration

The following is a sample configuration of a local audit in the `visiclt.ini` file:

```
[AUDIT_LOG]
;Audit log file
LOG_PATH="c:\myaudit.log"
[AUDIT_LOG_FILTERS]
;Including filter. It states that events with class id 1 and user DTM should
be logged.
LOG_FILTER="1;;;;;;;;;;;;DTM;;;;;0;1"
```

The following is a sample configuration of a filter refresh value in the `visi.ini` file:

```
[AUDIT_LOG]
; Refresh value in seconds
FILTER_REFRESH=40
```

PROJECT ID_AUDIT_MSGID Table

The following table describes the PROJECT ID_AUDIT_MSGID table, which specifies audit messages:

PROJECT ID_AUDIT_MSGID table		
Field	Type	Description
EVNT_MSGID	INT	ID of event class, type or message. Reserved ranges are as follows: <ul style="list-style-type: none">• 0 to 1000 is reserved for event class descriptions.• 1001 to 10000 is reserved for event type descriptions.• 10001 to 30000 is reserved for event descriptions.• 30001 to 59999 is reserved for event texts. Custom audit event ID ranges are as follows: <ul style="list-style-type: none">• 60000 to 61000 is reserved for custom event class descriptions.• 61001 to 70000 is reserved for custom event type descriptions.• 70001 to 90000 is reserved for custom event descriptions.• 90001 to 119999 is reserved for custom event texts.
EVNT_LANG_ID	INT	Language ID, which defines the language of the message class description.
EVNT_MSG_NAME	TEXT	Event class, type, or message description in the language defined by EVNT_LANG_ID.

S23_AUDIT_FILTER Table

The following table describes the S23_AUDIT_FILTER database table, which is used to set up audit configuration:

S23_AUDIT_FILTER table		
Name	Type	Description
EVNT_CLID	INT	Event class ID, reference to the event class name in the PROJECT ID_AUDIT_MSGID table.
EVNT_TPID	INT	Event type ID, reference to the event type in the PROJECT ID_AUDIT_MSGID table.
EVNT_SLID	INT	Severity level of the event. For information on severity levels, see Event Audit Data .
EVNT_MSGID	INT	Event message ID, reference to the event class name in the PROJECT ID_AUDIT_MSGID table.
EVNT_TRID	VARCHAR	Transaction ID this event is part of.
CNXT_WFID	INT	Workflow ID.
CNXT_PRID	VARCHAR[3]	Project ID.
CNXT_NDID	INT	Node ID.
CNXT_WIID	INT	Parcel ID.
CNXT_DOC	INT	Document ID.
CNXT_FOLDER	INT	Folder ID.
CNXT_SUBFOLDER	INT	Subfolder ID.
CNXT_UUID	VARCHAR[32]	User ID invoking the operation causing the event.
CNXT_TNID	VARCHAR	Tenant ID of the user.
CNXT_USID	INT	User session ID.
CNXT_WSTID	INT	User Exigen Workflow workstation ID.
EVNT_FILTER_TYPE	INT	Integer value: <ul style="list-style-type: none"> 0: including filter 1: excluding filter
EVNT_FILTER_STATE	INT	Integer value: <ul style="list-style-type: none"> 1: filter enabled 0: filter disabled
EVNT_FILTER_DESC	VARCHAR[254]	Description of the filter.
EVNT_FMTID	INT	Formatted text message ID.
CNTX_APP	VARCHAR[50]	Application name.
CNTX_BAT_ID	INT	Batch ID.
CNTX_OS_USER	VARCHAR[50]	User name in the form Domain\user, for example, Technology\Peter.

Audit Event Descriptions

This section describes audit events currently implemented in Exigen Workflow.

In audit event descriptions, class IDs indicate the following:

Audit events class ID	
ID	Description
0	Authentication.
1	Workflow operations.
2	Document operations.
3	Administration.
4	Indexing operations.

The following table lists currently implemented audit events and provides event class IDs, type IDs, event descriptions, and parameters:

Audit event description						
Class ID	Type ID	Message ID	Formatted text message ID	Description	Field name	Field description
0	1001	10005	30005	Successful user login	PARAM1	Exigen Workflow object name the user logged in to.
0	1001	10010	30010	Unsuccessful user login	PARAM1	Exigen Workflow object name to which user attempted login.
0	1002	10015	30015	User logout	PARAM1	Exigen Workflow object name from which the user logged out.
1	1003	10020	30020	Successful send operation	PARAM1	User ID to which parcel was sent.
					PARAM5	Exigen Workflow node ID that a parcel was sent from.
					PARAM10	Exigen Workflow node ID that a parcel was sent to.
1	1003	10300	30320	Successful distribute operation	PARAM1	User ID to which parcel was sent.
					PARAM2	User ID of previous parcel owner.
					PARAM5	Exigen Workflow node ID that a parcel was sent from.
					PARAM10	Exigen Workflow node ID that a parcel was sent to.

Audit event description						
Class ID	Type ID	Message ID	Formatted text message ID	Description	Field name	Field description
1	1003	10305	30325	Successful get from common operation	PARAM1	User ID to which the parcel was sent.
					PARAM2	User ID of the previous parcel owner.
					PARAM5	Exigen Workflow node ID that a parcel was sent from.
					PARAM10	Exigen Workflow node ID that a parcel was sent to.
2	1004	10025	30025	Task document view	PARAM1	Full path to DMS file.
					PARAM2	Parameter string for task program.
					PARAM3	Launched task name.
2	1004	10030	30030	DMS file view	PARAM1	Full path to DMS file.
2	1005	10035	30035	View of folder documents	No additional parameters.	
2	1006	10040	30040	View of parcel documents	No additional parameters.	
2	1007	10045	30045	Successful FTS processing start	PARAM1	Object name.
					PARAM2	Full path to document to be processed.
2	1007	10046	30046	Unsuccessful FTS processing start	PARAM1	Object name.
					PARAM2	Full path to document to be processed.
2	1008	10050	30050	Successful FTS processing finish	PARAM1	Object name.
					PARAM2	Full path to processed document.
2	1008	10051	30051	Unsuccessful FTS processing finish	PARAM1	Object name.
					PARAM2	Full path to processed document.
2	1009	10055	30055	Successful document opening	PARAM1	Object name.
					PARAM2	Full path to document file.
					PARAM5	Page number.
2	1009	10060	30060	Unsuccessful document opening	PARAM1	Object name.
					PARAM2	Full path to document file.
					PARAM5	Page number.
2	1009	10065	30065	Successful page OCR	PARAM1	Object name.
					PARAM2	Full path to document file.

Audit event description						
Class ID	Type ID	Message ID	Formatted text message ID	Description	Field name	Field description
2	1009	10070	30070	Unsuccessful page OCR	PARAM5	Page number.
					PARAM1	Object name.
					PARAM2	Full path to document file.
					PARAM5	Page number.
2	1009	10075	30075	Successful opening of file with recognized word list	PARAM1	Object name.
					PARAM2	Full path to the word list file.
					PARAM5	Error code of file operation.
2	1009	10080	30080	Unsuccessful opening of file with recognized word list	PARAM1	Object name.
					PARAM2	Full path to the word list file.
					PARAM5	Error code of file operation.
2	1010	10085	30085	Successful old FTS indexing	PARAM1	Object name.
					PARAM2	Full path to the document file.
2	1010	10090	30090	Unsuccessful old FTS indexing	PARAM1	Object name.
					PARAM2	Full path to the document file.
2	1010	10095	30095	Old FTS indexing is disabled	PARAM1	Object name.
					PARAM2	Full path to the document file.
2	1010	10100	30100	Successful fast FTS indexing	PARAM1	Object name.
					PARAM2	Full path to the document file.
2	1010	10105	30105	Unsuccessful fast FTS indexing	PARAM1	Object name.
					PARAM2	Full path to the document file.
2	1010	10110	30110	Fast FTS indexing is disabled	PARAM1	Object name.
					PARAM2	Full path to the document file.
2	1010	10115	30115	Successful main indexing	PARAM1	Object name.
					PARAM2	Full path to the document file.
2	1010	10120	30120	Unsuccessful main indexing	PARAM1	Object name.
					PARAM2	Full path to the document file.
2	1015	10130	30130	Document split	PARAM1	Full path to original DMS file.
					PARAM5	Original document deleted: <ul style="list-style-type: none"> 1: true 0: false
					PARAM10	Target RSN1.
					PARAM11	Target RSN2.

Audit event description						
Class ID	Type ID	Message ID	Formatted text message ID	Description	Field name	Field description
2	1020	10135	30135	Document merge	PARAM12	First page number in the range.
					PARAM13	Last page number in the range.
					PARAM1	Full path to original DMS file.
					PARAM5	Original document deleted: <ul style="list-style-type: none"> 1: true 0: false
					PARAM10	Target RSN.
2	1025	10140	30140	Document delete	PARAM12	Range start page number.
					PARAM13	Range end page number.
					PARAM1	Full path to DMS file.
					PARAM5	Page number.
					PARAM1	Full path to original DMS file.
2	1030	10145	30145	DMS page delete	PARAM5	Page number.
					PARAM1	Full path to original DMS file.
					PARAM1	Full path to the original DMS file.
					PARAM10	Page number of the first deleted page.
					PARAM11	Page number of the last deleted page.
2	1030	10146	30146	DMS page delete range	PARAM1	Full path to the original DMS file.
					PARAM10	Page number of the first deleted page.
					PARAM11	Page number of the last deleted page.
					PARAM1	Full path to the original DMS file.
					PARAM5	Target document RSN.
2	1035	10150		DMS page move	PARAM10	Page number in the original document.
					PARAM11	Page number in the target document.
					PARAM1	Full path to the original DMS file.
					PARAM5	Target document RSN.
					PARAM10	Page number in original document.
2	1040	10155	30155	DMS page copy	PARAM11	Page number in target document.
					PARAM1	Full path to the original DMS file.
					PARAM5	Target document RSN.
					PARAM10	Page number in original document.
					PARAM11	Page number in target document.
2	1045	10160	30160	DMS page undelete	PARAM1	Full path to original DMS file.
					PARAM5	Page number.
2	1050	10165	30165	Document split into	PARAM1	Full path to original DMS file.

Audit event description						
Class ID	Type ID	Message ID	Formatted text message ID	Description	Field name	Field description
				portions	PARAM5	Original document deleted: <ul style="list-style-type: none"> 1: true 0: false
					PARAM10	Target RSN.
					PARAM12	Range start page number.
					PARAM13	Range end page number.
2	1055	10170	30170	DMS rearrange	Rearrange is a sequence of operations with one transaction ID. Rearrange transaction can contain the following events: <ul style="list-style-type: none"> page copy page delete 	
					PARAM1	Path to document file.
					PARAM5	Target document ID.
					PARAM10	Original document deleted: <ul style="list-style-type: none"> 1: true 0: false
2	1185	10330	30355	DMS page add	PARAM1	Full path to original DMS file.
					PARAM10	Start page number of added pages.
					PARAM11	End page number of added pages.
2	1190	10335	30360	DMS page rescan	PARAM1	Full path to original DMS file.
					PARAM10	Start page number of added pages.
					PARAM11	End page number of added pages.
2	1065	10180	30180	DMS page rescan all	PARAM1	Full path to original DMS file.
				Note: Audit events concerning DMS page modifications in the Scan dialog are saved in the audit table only if the user saves the modified DMS file.	PARAM5	Page number.
2	1070	10185	30185	DMS file object modify	PARAM1	Full path to DMS file.
					PARAM2	Object type description.
					PARAM5	Document page number.

Audit event description						
Class ID	Type ID	Message ID	Formatted text message ID	Description	Field name	Field description
2	1075	10190	30190	DMS file object add	PARAM1	Full path to DMS file.
					PARAM2	Object type description.
					PARAM5	Document page number.
2	1080	10195	30195	DMS file object delete	PARAM1	Full path to DMS file.
					PARAM2	Object type description.
					PARAM5	Document page number.
2	1085	10200	30200	DMS file object content modify	PARAM1	Full path to DMS file.
					PARAM2	Object type description.
					PARAM5	Document page number.
2	1090	10205	30205	DMS file object content add	PARAM1	Full path to DMS file.
					PARAM2	Object type description.
					PARAM5	Document page number.
2	1095	10210	30210	DMS file object content delete	PARAM1	Full path to the DMS file.
					PARAM2	Object type description.
					PARAM5	Document page number.
2	1115	10235		Printing a DMS document from the Image Viewer	No additional parameters.	
2	1120	10240		Emailing a DMS document from the Image Viewer	No additional parameters.	
2	1125	10245		EWf Web checkout document	No additional parameters.	
2	1130	10250		EWf Web check in document	PARAM5	<ul style="list-style-type: none"> 0: checked in 1: checkin undone
2	1135	10255		EWf Web continue editing of checked out document	No additional parameters.	
1	1145	10265		Server object started	PARAM1	Object name.
					PARAM5	<ul style="list-style-type: none"> 0: run in regular server mode 1: run as a service

Audit event description						
Class ID	Type ID	Message ID	Formatted text message ID	Description	Field name	Field description
1	1150	10270		Server object closed	PARAM1	Object name.
					PARAM5	<ul style="list-style-type: none"> 0: run in regular server mode 1: run as a service
1	1155	10275	30275	Create parcel	PARAM5	Reserved for subformats.
1	1155	10275	30280	Create parcel by split	PARAM5	Source parcel ID.
1	1155	10275	30285	Create parcel by merge	PARAM5	Reserved for subformats.
1	1160	10280	30290	Delete parcel	PARAM5	Reserved for subformats.
1	1160	10280	30295	Delete parcel by split	PARAM5	Reserved for subformats.
1	1160	10280	30300	Delete parcel by merge	PARAM5	Target parcel ID.
1	1165	10285	30305	Split parcel	PARAM5	Count of new parcels created by split operation.
1	1170	10290	30310	Merge parcel	PARAM5	Count of merged parcels.
2	1175	10310	30330	Request to print document	PARAM1	Device name.
					PARAM5	Status of cover page: <ul style="list-style-type: none"> 1: attached 0: not attached
					PARAM6	Print job priority: <ul style="list-style-type: none"> 0: no priority 1: low 2: normal 3: high
					PARAM7	Exigen Workflow Print Job ID.
					PARAM10	Range start page number.
					PARAM11	Range end page number.
					PARAM12	Number of copies.
					PARAM13	Print mode: <ul style="list-style-type: none"> 0: original 1: with overlays
2	1175	10295	30315	Print document	PARAM1	Printer or device name.
					PARAM5	Status of cover page: <ul style="list-style-type: none"> 1: attached 0: not attached
					PARAM10	Range start page number.
					PARAM11	Range end page number.

Audit event description						
Class ID	Type ID	Message ID	Formatted text message ID	Description	Field name	Field description
					PARAM12	Number of copies.
					PARAM13	Print mode: <ul style="list-style-type: none"> 0: original 1: with overlays
2	1175	10295	30335	Print document Note: This event occurs when printing is performed by Print Server.	PARAM3	Requester user ID.
3	1180	10320	30345	Successful database server login password change Note: This event occurs when extended security is ON.	PARAM1	Affected user ID.
					PARAM4	Database name.
3	1180	10325	30350	Unsuccessful database server login password change Note: This event occurs when extended security is ON.	PARAM1	Affected user ID.
					PARAM2	Error description.
					PARAM4	Database name.
3	1210	10370	30380	Audit event delete	PARAM5	Time setting: <ul style="list-style-type: none"> 0: local time 1: server time
					PARAM9	Delete audit events older than specified date.
3	1210	10372	30382	Audit event export	PARAM5	Time setting: <ul style="list-style-type: none"> 0: local time 1: server time
					PARAM8	Export events newer than specified date.
					PARAM9	Export events older than specified date.
3	1180	10340	30365	User create	PARAM1	Affected user ID.
3	1180	10341	30366	User delete	PARAM1	Affected user ID.

Audit event description						
Class ID	Type ID	Message ID	Formatted text message ID	Description	Field name	Field description
3	1180	10342	30367	User modify	PARAM1	Affected user ID.
3	1180	10343	30368	User security level change	PARAM1	Affected user ID.
					PARAM5	Previous security level ID.
3	1180	10346	30371	User password change	PARAM1	Affected user ID.
3	1180	10347	30372	User disable	PARAM1	Affected user ID.
3	1180	10348	30373	User enable	PARAM1	Affected user ID.
3	1182	10360	30380	Security level create	PARAM1	Created level name.
					PARAM5	Created level ID.
3	1182	10361	30381	Security level delete	PARAM1	Deleted level name.
					PARAM5	Deleted level ID.
3	1182	10362	30382	Security level modify	PARAM1	Modified level name.
					PARAM5	Modified level ID.
3	1182	10370	30390	Document context security level create	PARAM1	Created level name.
					PARAM5	Created level ID.
3	1182	10371	30391	Document context security level delete	PARAM1	Deleted level name.
					PARAM5	Deleted level ID.
3	1182	10372	30392	Document context security level modify	PARAM1	Modified level name.
					PARAM5	Modified level ID.
3	1181	10380	30400	Global group create	PARAM1	Created group name.
					PARAM5	Created group ID.
3	1181	10381	30401	Global group delete	PARAM1	Deleted group name.
					PARAM5	Deleted group ID.
3	1181	10382	30402	Global group modify	PARAM1	Modified group name.
					PARAM5	Modified group ID.
3	1181	10385	30405	Folder group create	PARAM1	Created group name.

Audit event description						
Class ID	Type ID	Message ID	Formatted text message ID	Description	Field name	Field description
3	1181	10386	30406	Folder group delete	PARAM5	Created group ID.
					PARAM1	Deleted group name.
					PARAM5	Deleted group ID.
3	1181	10387	30407	Folder group modify	PARAM1	Modified group name.
					PARAM5	Modified group ID.
3	1181	10390	30410	Workflow group create	PARAM1	Created group ID.
					PARAM5	Created group description.
3	1181	10391	30411	Workflow group delete	PARAM1	Deleted group ID.
					PARAM5	Deleted group description.
3	1181	10392	30412	Workflow group modify	PARAM1	Modified group ID.
					PARAM5	Modified group description.
3	1180	10404	30424	Successful database server login create	PARAM1	Affected user ID.
					PARAM4	Database name.
					PARAM5	Login type: <ul style="list-style-type: none"> 0: database server login 1: Windows NT user
3	1180	10406	30426	Unsuccessful database server login create	PARAM1	Affected user ID.
					PARAM2	Error description.
					PARAM4	Database name.
					PARAM5	Login type: <ul style="list-style-type: none"> 0: database server login 1: Windows NT user
3	1180	10408	30428	Successful database server login delete	PARAM1	Affected user ID.
					PARAM4	Database name.
					PARAM5	Login type: <ul style="list-style-type: none"> 0: database server login 1: Windows NT user
3	1180	10410	30430	Unsuccessful database server login delete	PARAM1	Affected user ID.
					PARAM2	Error description.

Audit event description						
Class ID	Type ID	Message ID	Formatted text message ID	Description	Field name	Field description
3	1180	10412	30432	Successful database user create	PARAM4	Database name.
					PARAM5	Login type: <ul style="list-style-type: none"> 0: database server login 1: Windows NT user
					PARAM1	Affected user ID.
					PARAM4	Database name.
					PARAM5	User: <ul style="list-style-type: none"> 0: database user 1: Windows NT user
3	1180	10414	30434	Unsuccessful database user create	PARAM1	Affected user ID.
					PARAM2	Error description.
					PARAM4	Database name.
					PARAM5	User: <ul style="list-style-type: none"> 0: database user 1: Windows NT user
3	1180	10416	30436	Successful database user delete	PARAM1	Affected user ID.
					PARAM4	Database name.
					PARAM5	User: <ul style="list-style-type: none"> 0: database user 1: Windows NT user
3	1180	10418	30438	Unsuccessful database user delete	PARAM1	Affected user ID.
					PARAM2	Error description.
					PARAM4	Database name.
					PARAM5	User: <ul style="list-style-type: none"> 0: database user 1: Windows NT user
3	1180	10420	30440	Successfully added database user to database role	PARAM1	Affected user ID.
					PARAM3	Database role name.
					PARAM4	Database name.

Audit event description						
Class ID	Type ID	Message ID	Formatted text message ID	Description	Field name	Field description
3	1180	10422	30442	Unsuccessfully added database user to database role	PARAM5	User: <ul style="list-style-type: none"> 0: database user 1: Windows NT user
					PARAM1	Affected user ID.
					PARAM2	Error description.
					PARAM3	Database role name.
					PARAM4	Database name.
3	1180	10424	30444	Successfully added database server login to server role	PARAM5	User: <ul style="list-style-type: none"> 0: database user 1: Windows NT user
					PARAM1	Affected user ID.
					PARAM3	Server role name.
					PARAM4	Database name.
					PARAM5	Login: <ul style="list-style-type: none"> 0: database server 1: Windows NT user
3	1180	10426	30446	Unsuccessfully added database server login to server role	PARAM1	Affected user ID.
					PARAM2	Error description.
					PARAM3	Server role name.
					PARAM4	Database name.
					PARAM5	Login: <ul style="list-style-type: none"> 0: database server 1: Windows NT user
2	1212	10428	30448	Document add	PARAM1	Full path to the document file.
3	1180	10430	30450	Successfully removed database user from database role	PARAM1	Affected user ID.
					PARAM3	Database role name.
					PARAM4	Database name.

Audit event description						
Class ID	Type ID	Message ID	Formatted text message ID	Description	Field name	Field description
3	1180	10432	30452	Unsuccessfully removed database user from database role	PARAM5	User: <ul style="list-style-type: none"> 0: database user 1: Windows NT user
					PARAM1	Affected user ID.
					PARAM2	Error description.
					PARAM3	Database role name.
					PARAM4	Database name.
3	1180	10434	30454	Successfully removed database server login from server role	PARAM5	User: <ul style="list-style-type: none"> 0: database user 1: Windows NT user
					PARAM1	Affected user ID.
					PARAM3	Server role name.
					PARAM4	Database name.
					PARAM5	Login: <ul style="list-style-type: none"> 0: database server 1: Windows NT user
3	1180	10436	30456	Unsuccessfully removed database server login from server role	PARAM1	Affected user ID.
					PARAM2	Error description.
					PARAM3	Server role name.
					PARAM4	Database name.
					PARAM5	Login: <ul style="list-style-type: none"> 0: database server 1: Windows NT user
3	1180	10438	30458	Add user to workflow group	PARAM1	Affected user ID.
					PARAM3	Workflow group ID.
3	1180	10440	30460	Remove user from workflow group	PARAM1	Affected user ID.
					PARAM3	Workflow group ID.
3	1180	10442	30462	Add user to folder group	PARAM1	Affected user ID.
					PARAM3	Folder group ID.
3	1180	10444	30464	Remove user from	PARAM1	Affected user ID.

Audit event description						
Class ID	Type ID	Message ID	Formatted text message ID	Description	Field name	Field description
				folder group	PARAM3	Folder group ID.
3	1180	10446	30466	Add user to global group	PARAM1	Affected user ID.
					PARAM3	Global group ID.
3	1180	10448	30468	Remove user from global group	PARAM1	Affected user ID.
					PARAM3	Global group ID.
3	1180	10450	30470	Add global group to global group	PARAM1	Affected user ID.
					PARAM3	Global group ID.
3	1180	10452	30472	Remove global group from global group	PARAM1	Affected user ID.
					PARAM3	Global group ID.
4	1238	10498	30498	Folder create	PARAM5	Folder ID.
4	1240	10500	30500	Folder delete	PARAM5	Folder ID.
4	1222	10482	30482	Folder fields modify	PARAM5	Folder ID.
4	1242	10502	30502	Subfolder create	PARAM5	Subfolder ID.
4	1244	10504	30504	Subfolder delete	PARAM5	Subfolder ID.
4	1224	10484	30484	Subfolder fields modify	PARAM5	Subfolder ID.
4	1246	10506	30506	Document type create	PARAM1	Document type ID.
4	1248	10508	30508	Document type delete	PARAM1	Document type ID.
4	1250	10510	30510	Document type modify	PARAM1	Old document type ID.
					PARAM2	New document type ID.
4	1226	10486	30486	Assign parcel to folder	PARAM5	Folder ID to which the parcel is assigned.

Audit event description						
Class ID	Type ID	Message ID	Formatted text message ID	Description	Field name	Field description
4	1228	10488	30488	Assign document to subfolder	PARAM5	Subfolder ID to which the document is assigned.
4	1230	10490	30490	Assign document to document type	PARAM1	Document type ID to which the document is assigned.
					PARAM2	Previous document type.
4	1232	10492	30492	Assign subfolder to folder	PARAM5	Subfolder ID.
					PARAM10	Folder ID.
4	1234	10494	30494	Parcel fields modify	No additional parameters.	
4	1236	10496	30496	Document fields modify	No additional parameters.	
2	1220	10480	30480	Document scan	PARAM1	Full path to a DMS file.
					PARAM5	Mode: <ul style="list-style-type: none"> 0: scanning performed 1: scanning canceled
2	1252	10512	30512	E-mail document	PARAM1	Full path to the document file.
					PARAM4	Attached file extension.
					PARAM5	Document ID.
					PARAM10	Start page number.
					PARAM11	End page number.
					PARAM12	Attachment status: <ul style="list-style-type: none"> 0: document file attached 1: no document file attached
2	1252	10514	30514	E-mail parcel	PARAM5	Parcel ID.
					PARAM13	Attachment status: <ul style="list-style-type: none"> 0: document file attached 1: no document file attached
2	1252	10516	30516	E-mail folder	PARAM5	Folder ID.

Audit event description						
Class ID	Type ID	Message ID	Formatted text message ID	Description	Field name	Field description
2	1252	10518	30518	Original document view	PARAM1	Full path to the original document file.
2	1254	10520	30520	Document has no pages	PARAM1	Full path to the document.
2	1254	10522	30522	Document page extract failed	PARAM1	Full path to the document.
					PARAM5	Page number.
2	1256	10524	30524	File open failed	PARAM1	Full path to the document.
2	1256	10526	30526	File conversion failed	PARAM1	Full path to the document.
					PARAM2	Error description.
					PARAM4	Conversion target file extension.
2	1256	10528	30528	File copy failed	PARAM1	Full path to source file.
					PARAM2	Full path to destination file.
2	1256	10530	30530	File read failed	PARAM1	Full path to the file.
1	1264	10542	30542	Parcel export failed due to already existing identification in target	PARAM4	Target project ID.
1	1264	10542	30544	Parcel export failed due to rule violation	PARAM4	Target project ID.
5	1262	10536	30536	Connect to database failed	PARAM1	Database login name, which attempted to connect to the database.
					PARAM2	Error description.
					PARAM4	Database name.
1	1003	10538	30538	Unsuccessful send operation	PARAM1	User ID of user to whom the parcel is sent.
					PARAM5	Workflow node ID from which the parcel is sent.
					PARAM10	Workflow node ID to which the parcel is sent.
2	1264	10540	30530	Document export failed due to already existing identification in target	PARAM1	Full path to file.
					PARAM4	Target project ID.
1	1260	10534	30534	Server initialization failed due to incorrect configuration	PARAM1	Error description.
2	1256	10544	30546	File create failed	PARAM1	Full path to file.
					PARAM3	Error description if available.
2	1256	10546	30548	File save failed	PARAM1	Full path to file.

Audit event description						
Class ID	Type ID	Message ID	Formatted text message ID	Description	Field name	Field description
2	1256	10548	30550	File write failed	PARAM3	Error description if available.
					PARAM1	Full path to file.
					PARAM3	Error description if available.
2	1256	10550	30552	File close failed	PARAM1	Full path to file.
					PARAM3	Error description if available.
2	1256	10552	30554	File delete failed	PARAM1	Full path to file.
					PARAM3	Error description if available.
2	1268	10556	30558	Document copy	PARAM1	Full path to the document file.
					PARAM4	Extension of the copied document file.
					PARAM5	Document ID.
					PARAM12	Document file status: <ul style="list-style-type: none"> 0: document file copied 1: document file not copied
					PARAM13	Document attribute status: <ul style="list-style-type: none"> 0: document attributes copied 1: document attributes not copied
1	1003	10558	30560	Successful reassign operation	PARAM1	User ID to which parcel was sent.
					PARAM2	User ID of previous parcel owner.
					PARAM5	Workflow node ID from which parcel is sent.
					PARAM10	Workflow node ID to which parcel is sent.
1	1171	10291	30311	Hold Parcel	PARAM8	Parcel activation date in the database server time zone.
1	1172	10292	30312	Activate Parcel	PARAM8	Planned activation date for parcel in the database server time zone.
2	1256	10602	30584	File format unsupported	PARAM1	Full path to file.
					PARAM5	Page number. If not available, NULL must be set.
1	1266	10554	30556	Task instance status change	PARAM5	Status ID.
					PARAM10	Previous status ID.
1	1266	10560	30562	Create task instance	No additional parameters.	

Audit event description						
Class ID	Type ID	Message ID	Formatted text message ID	Description	Field name	Field description
1	1266	10562	30564	Delete task instance	No additional parameters.	
1	1266	10564	30566	Modify task instance	No additional parameters.	
1	1266	10566	30568	Cancel task instance status change	PARAM5 PARAM10	Status ID. Previous status ID.
1	1266	10568	30570	Reassign task instance	PARAM1	User ID to which task instance is reassigned.
1	1266	10570	30572	Add task instance attachment	PARAM5	Attached document ID.
1	1266	10572	30574	Remove task instance attachment	PARAM5	Removed document ID.
1	1266	10574	30576	Create taskflow instance	PARAM5	Taskflow instance ID.
1	1266	10576	30578	Delete taskflow instance	PARAM5	Taskflow instance ID.
1	1266	10578	30580	Modify taskflow instance	PARAM5	Taskflow instance ID.
1	1266	10600	30582	Escalation of task instance	PARAM1 PARAM2 PARAM5 PARAM8	User ID before escalation. User ID after escalation. Taskflow instance ID. Escalation due date and time.
2	1270	10604	30586	Document zones processed	PARAM1	Full path to the original DMS file.
					PARAM4	Document type.
					PARAM5	Total count of processed zones.
					PARAM8	Date and time when process is started.
					PARAM9	Date and time when process is completed.
					PARAM10	Total count of low confidence zones.
					PARAM11	Total count of medium confidence zones.
					PARAM12	Total count of high confidence zones.
2	1270	10606	30588	Document zones changed	PARAM13	Total count of forced QA zones.
					PARAM1	Full path to the original DMS file.
					PARAM4	Document type.

Audit event description						
Class ID	Type ID	Message ID	Formatted text message ID	Description	Field name	Field description
					PARAM5	Total count of processed zones.
					PARAM8	Date and time when process is started.
					PARAM9	Date and time when process is completed.
					PARAM10	Total count of low confidence zones.
					PARAM11	Total count of medium confidence zones.
					PARAM12	Total count of high confidence zones.
					PARAM13	Total count of forced QA zones.
2	1270	10608	30590	Document characters processed	PARAM1	Full path to the original DMS file.
					PARAM4	Document type.
					PARAM5	Total count of processed zones.
					PARAM8	Date and time when process is started.
					PARAM9	Date and time when process is completed.
					PARAM10	Total count of low confidence zones.
					PARAM11	Total count of medium confidence zones.
					PARAM12	Total count of high confidence zones.
					PARAM13	Total count of forced QA zones.
2	1270	10610	30592	Document characters changed	PARAM1	Full path to the original DMS file.
					PARAM4	Document type.
					PARAM5	Total count of processed zones.
					PARAM8	Date and time when process is started.
					PARAM9	Date and time when process is completed.
					PARAM10	Total count of low confidence zones.

Audit event description						
Class ID	Type ID	Message ID	Formatted text message ID	Description	Field name	Field description
					PARAM11	Total count of medium confidence zones.
					PARAM12	Total count of high confidence zones.
					PARAM13	Total count of forced QA zones.
2	1271	10612	30594	Document rejected	PARAM1	Full path to the original DMS file.
					PARAM4	Document type.
2	1271	10614	30596	Template page linked	PARAM1	Full path to the original DMS file.
					PARAM2	Full path to the template file.
					PARAM4	Document type.
					PARAM5	Template ID.
					PARAM10	Document page number.
2	1214	10429	30449	New document version created	PARAM11	Template page number.
					PARAM14	Full path to the document file.
2	1273	10616	30598	Document version set as active	PARAM1	Version ID.
					PARAM11	Full path to the document file.
2	1027	10142	30142	Document version deleted	PARAM11	Parent version ID.
					PARAM14	Version ID.
2	1256	10525	30525	Document file cannot be destroyed	PARAM1	Full path to the document file.
					PARAM14	Error description if available.
					PARAM2	Version ID.
2	1275	10618	30600	Document or version content is recycled	PARAM1	Full path to the document file.
					PARAM14	Version ID.
2	1026	10141	30141	Document record is deleted from the DOC_RECYCLE table and document file is removed	PARAM1	Full path to the document file.
					PARAM2	Document commit ID.
					PARAM5	Commit configuration ID.
2	1028	10143	30143	Document version record is deleted from the DOC_RECYCLE table and document file is removed	PARAM1	Full path to the document file.
					PARAM2	Document commit ID.
					PARAM5	Commit configuration ID.
					PARAM14	Version ID.
2	1029	10144	30144	Document version is destroyed	PARAM1	Full path to the document file.
					PARAM2	Document commit ID.

Audit event description						
Class ID	Type ID	Message ID	Formatted text message ID	Description	Field name	Field description
2	1024	10139	30139	Document is destroyed	PARAM5	Commit configuration ID.
					PARAM14	Version ID.
					PARAM1	Full path to the document file.
					PARAM2	Document commit ID.
					PARAM5	Commit configuration ID.





Audit Server



Events with the identifiers 1070, 1075, 1080, 1085, 1090, and 1095 store audit data in DMS files. Audit Server synchronizes the DMS file audit data with the common Exigen Workflow audit mechanism.

To set up Audit Server, proceed as follows:

1. In Workflow Explorer, start Audit Server.
2. Click **Process Setup** or select **Run > Process Setup**.
3. To keep the server running after starting, select the **Keep running after started** check box.
4. In the **Audit Type** box, select one of the following options:
 - To write DMS Viewer actions in the same way as user actions in a database, select **Use Audit Project Tables**.
 - To convert old-style audit files or to import them into a database, select **Use DMS Viewer Audit Files**.
5. To register only those DMS Viewer events that apply to the filters set in the Administrator utility, select **Use Audit Event Filters**.
6. Click **OK**.

Audit Server window buttons and menu commands are described in the following table:

Audit Server buttons and menu commands			
Button	Shortcut key	Menu commands	Description
	F3	Run > Process Setup	Specifies the process interval and audit type.
	F2	File > Save Configuration	Saves the window configuration.
		Run > Start Server	Starts Audit Server.
		Run > Stop Server	Stops Audit Server.

Audit Server buttons and menu commands			
Button	Shortcut key	Menu commands	Description
	F1	Help > Context Help	Displays context-sensitive help.
	CTRL+F1	Help > Help Topics	Displays a list of help topics.
		Help > About Exigen Workflow	Displays the Exigen Workflow version, copyright information, and the current workstation ID.
	F12	File > Exit	Exits Audit Server.

To enable DMS audit file generation by DMS viewer, add the following section to the `visi.ini` file:

```
[VIEWAUDIT]
LOCATION=C:\AUDIT
```

When scanning, opening, printing or opening and modifying DMS files, `Username.AUD` files are generated with the following information:

```
DTM,777,Fri Jan 25 15:52:46 2002,C:\DMS_SCAN\DTM\00000072.DMS,Opened.
DTM,777,Fri Jan 25 15:52:57 2002,C:\DMS_SCAN\DTM\00000072.DMS,Modified.
DTM,777,Fri Jan 25 15:52:57 2002,C:\DMS_SCAN\DTM\00000073.DMS,Opened.
DTM,777,Fri Jan 25 15:53:05 2002,C:\DMS_SCAN\DTM\00000073.DMS,Modified.
```

Appendix E: Diagnoses

The following table describes E-Capture diagnoses codes:

E-Capture diagnoses codes	
Message	Definition
NOT_VALID_FIELD	Field not valid.
VENDOR_ISSUE	Vendor not recognized.
PAGES_IN_FILE	Incorrect control information about the number of pages in a compound document.
IDENTIFIER_NUMBER	Incorrect control information about the label of the processed compound document.
NO_FORMS_IN_FILE	No recognized forms inside the processed document.
EMPTY_MANDATORY_FIELD	Field that must contain information is blank.
WRONG_CALCULATONS	Incorrect calculation within a processed document.
NO_FORM_SCHEDULE	Schedule of Forms is not found.
FORM_COMPLETENESS	One or more of the forms listed on the Schedule of Forms is not found.
SOURCE_FILE_NAME	In the event of a problem, this diagnosis places the source file name in the destination Exigen Workflow field.
NO_REC_IN_REF_TABLE	No recognized records in the reference table.

Appendix F: ScriptCalls

The following table describes predefined E-Capture ScriptCalls:

Predefined E-Capture ScriptCalls		
Name	Common function	Default behavior
AssignDocTypes	Assigns Exigen Workflow document types based on extracted content information.	Assigns the policy type to the Exigen Workflow document field type.
CheckFormCompleteness	Confirms if all forms listed on the Schedule of Forms are contained within the document.	Checks whether the forms listed in a particular Schedule of Forms are in a document.
DefinePolicyTypes	Determines policy types based on extracted control information from control records or files.	Locates a specific control record to determine policy type.
ExtDataFromSchedOfLoc	Extracts information from a Schedule of Locations.	Extracts data from a particular Schedule of Locations.
ExtFormScheduleEntireData	Prepares a final list of required forms within a document.	Combines data from all the pages of the Schedule of Forms and Endorsements.
ExtFormSchedulePageData	Extracts information from a selected page of the Schedule of Forms.	Extracts data from a selected page for a particular Schedule of Forms.
ExtNamedInsured	Extracts information from the Schedule of Named Insured.	Extracts data from a particular Schedule of Named Insured.
ExtractLegacyIndexData	Extracts information from a custom table based on a set of custom conditions.	Extracts legacy data from a specific reference table.
ProcessControlFile	Processes information contained in the control file.	Reads the specific control file as text and extracts the policy type, vendor, and number of pages in the document.
ProcessControlRecord	Processes information contained on the first page of a PCL file.	Reads the specific control record as text and extracts the policy type, vendor and number of pages in the document.
ProcessFileName	Processes a file name.	No action by default.
ProcessUnrecognizedFile	Provides processing instructions if no mandatory control information is specified.	Inserts default policy type.
ScriptProcessCriticalError	Reacts to critical errors in processing. Critical errors include the following: VENDOR_ISSUE FORM_COMPLETENESS WRONG_CALCULATIONS NO_FORMS_IN_FILE	Places the appropriate message in an Exigen Workflow database field.

Predefined E-Capture ScriptCalls		
Name	Common function	Default behavior
	NO_FORM_SCHEDULE NO_VALID_FIELD EMPTY_MANDATORY_FIELD	
SetInfo	Receives information about E-Capture Server setup and the results of preprocessing, and makes it available to other scripts.	No action by default.
TransformField	Transforms extracted field into the required output.	No action by default.
TransRefTableCondition	Transforms original conditions into SQL query conditions.	Eliminates dashes from the set of conditions.
TransformIndexRow	Changes Exigen Workflow folder, subfolder and document fields.	Combines different documents related to the same policy into one folder.
TriggerIndexRow	Initiates actions required by registered trigger forms.	Registered trigger forms assign document type.
UpdateFolder	Updates folder name.	Transforms data as required by registered trigger forms.
ValidateField	Validates standard and customized fields, such as TELEPHONE, ADDRESS, ZIPCODE, STRING(3,8), NUMBER(15,18).	Validates the following field types: date, date/time, integer, number, and time.

Appendix G: Exigen Workflow User Authentication Mechanism

Exigen Workflow user authentication is based on two settings:

- [Authentication Mode](#)
- [Database Connection Mode](#)

The following additional topics are described in this section:

- [Available Configurations for the Authentication and Database Connection Modes](#)
- [Switching between Database Users](#)
- [Multiple Database Servers and Database Authentication](#)
- [Performing a Single Login](#)
- [Performing a Trusted Login](#)

Authentication Mode

Authentication mode specifies how the user is authenticated in the Exigen Workflow system. The following table describes the available authentication modes:

Authentication modes		
Mode	Short name	Description
EWf	V	Authentication by Exigen Workflow.
Win32	W	Authentication through Win32. The mode is implemented in Exigen Workflow Web.
CCID Win32	C	Authentication by the current Windows user identity.
Database	D	Authentication by the database. This authentication mode is available only in systems that have extended security enabled as described in <i>Exigen Workflow Installation Guide</i> , Chapter 2: Installing Exigen Workflow, Creating or Upgrading the Exigen Workflow Database Structure.
Genesys	G	Authentication by Exigen Workflow.

Database Connection Mode

The database connection mode determines how the user is connected to the database. The following table describes the available database connection modes:

Database connection modes		
Name	Short name	Connection method
visi.ini	V	Login user ID and password from the <code>visi.ini</code> file.
Login	L	Login user ID and password from the login window or parameters. This connection mode is available only in systems that have extended security enabled as described in <i>Exigen Workflow Installation Guide</i> , Chapter 2: Installing Exigen Workflow, Creating or Upgrading the Exigen Workflow Database Structure.
Trusted	T	Windows trusted connection by client Win32 identity. This connection mode is available only in systems that have extended security enabled as described in <i>Exigen Workflow Installation Guide</i> , Chapter 2: Installing Exigen Workflow, Creating or Upgrading the Exigen Workflow Database Structure.

If database authentication is specified, Exigen Workflow verifies whether the user has access to the required database.

Exigen Workflow offers database authentication for the following databases:

- SQL Server
- Oracle

For each database, a user can be assigned one of two roles as described in the following table:

User database roles	
Role	Description
User	Reads table data.
Administrator	Creates tables and maintains table fields.

Database Permissions

Database permissions differ depending on the database used. The following table lists database permissions for SQL Server:

SQL Server database permissions		
Role	Permission	Permission type
User	db_datareader	Fixed database role.
	db_datawriter	Fixed database role.
Administrator	db_owner	Fixed server role.

The following table lists database permissions for Oracle databases:

Oracle database permissions	
Role	Permissions
User	CREATE SESSION
	ALTER SESSION
	SELECT, INSERT, DELETE, and UPDATE for Exigen Workflow system tables

Oracle database permissions	
Role	Permissions
Administrator	SELECT, INSERT, DELETE, and UPDATE for Exigen Workflow project tables, views, and sequences
	SELECT for Exigen Workflow system views
	ALTER ANY CLUSTER
	ALTER ANY INDEX
	ALTER ANY PROCEDURE
	ALTER ANY SEQUENCE
	ALTER ANY TABLE
	ALTER ANY TRIGGER
	ALTER SESSION
	ALTER USER
	CREATE ANY CLUSTER
	CREATE ANY INDEX
	CREATE ANY PROCEDURE
	CREATE ANY SEQUENCE
	CREATE ANY TABLE
	CREATE ANY TRIGGER
	CREATE ANY VIEW
	CREATE ROLE
	CREATE SESSION
	CREATE USER
	DROP ANY CLUSTER
	DROP ANY INDEX
	DROP ANY PROCEDURE
	DROP ANY SEQUENCE
	DROP ANY TABLE
	DROP ANY TRIGGER
	DROP ANY VIEW
	DROP USER
	EXECUTE ANY PROCEDURE
	SELECT_CATALOG_ROLE
	SELECT ON "SYS"."V_\$SESSION"
	SELECT ON "SYS"."DBA_ROLE_PRIVS"
	SELECT ON "SYS"."DBA_ROLES"
	ALL for Exigen Workflow system tables
	ALL for Exigen Workflow project tables, views, and sequences
	SELECT for Exigen Workflow system views
	All permissions assigned to users: vusers

Implementing Database Authentication

This section describes the following procedures to ensure that database authentication functions properly:

- [Specifying Database Permissions](#)
- [Viewing and Correcting Project Errors](#)
- [Specifying Database Authentication and Setting the Database Connection Mode](#)

Specifying Database Permissions

After installing Exigen Workflow, to specify database permissions, proceed as follows:

1. Verify user privileges for the database by using a database administration tool.

For information on user privileges for SQL and Oracle databases, see [Required Privileges for SQL and Oracle Databases](#).

2. If a user lacks required privileges, add the privileges using the database administration tool.
3. To open the **Workflow Database Installation/Upgrade Wizard** dialog, select **Start > Programs > Exigen Solution > Exigen Workflow > Workflow Database Startup**.

The **Workflow Database Installation/Upgrade Wizard** dialog appears.

4. In the **Database** field, enter the database name.
5. In the **User** field, enter the database user ID.
6. In the **Password** field, enter the database password.
7. Click **Connect**.
8. Select **Use extended security**.
9. Click **Run**.
10. Click **Log File**.

The log file appears.

11. In the log file, locate `vfadmins` and `vfusers`.
12. Verify that `vfadmins` and `vfusers` have the required permissions.

For information on required permissions, see [Database Permissions](#).

13. If the `vfadmins` and `vfusers` do not have the required permissions, check the log file to troubleshoot the lack of permissions.
14. To set user or administrator database permissions, in Exigen Workflow Explorer, select **Administration Tools > Workflow Tools > Administrator**.
15. Double click the **Administrator** icon.
16. In the **Administrator Utilities** window, select **Administrator > System Setup**.

17. In the **System Setup** window, select **Setup > Security Levels**.
18. In the **Levels** tab, double click the name of the appropriate user.
19. In the **Modify Level** window, click the arrow in the **Database Role** field and select **User** or **Administrator**.
20. Click **OK**.
21. In the **Security Level Setup** window, click **Close**.

Viewing and Correcting Project Errors

To view and correct project errors, proceed as follows:

1. In Exigen Workflow Explorer, select **Database Tools > Project Builder**.
2. Double click the **Project Builder** icon.
3. In the **Project Builder** window, select a project.
4. Select **Project > Check Project Version**.
5. If errors are displayed in the **Check Project Version** dialog, double click the corresponding line to correct the errors.
6. When all errors are corrected, click **Close**.
7. For each project, repeat steps 3-5.

Specifying Database Authentication and Setting the Database Connection Mode

To specify database authentication and set the database connection mode, proceed as follows:

1. In the `INI` subfolder of the Exigen Workflow system folder, open the `visiclt.ini` file.
2. In the `General` Section, under `[winclient]`, enter the following lines:

```
authentication_mode=D
```

```
db_connection_mode=L
```

For information on selecting a database connection mode, see [Database Connection Mode](#).

3. Save and close the `visiclt.ini` file.

Required Privileges for SQL and Oracle Databases

The following privileges are required for database authentication using SQL Server:

- The login ID must be a member of the `securityadmin` fixed server role.
- The database user associated with the login ID must be a member of the `db_owner` fixed database role.

The following privileges are required for database authentication using an Oracle database:

- Administrator privileges for Oracle must be available.

For a list of administrator privileges, see [Database Permissions](#).

- SELECT privileges on SYS schema objects must be granted using the `GRANT` option. This operation is performed using a database tool.

If there are projects outside the master database, users must have appropriate privileges in each database.

Available Configurations for the Authentication and Database Connection Modes

The Exigen Workflow system allows you to use authentication mode and database connection mode in the following configurations:

Available configurations	
Authentication mode	Database connection mode
EWF	<code>Visi.ini</code>
CCID Win32	<code>Visi.ini</code>
CCID Win32	Trusted
Database	Login
Genesys	<code>Visi.ini</code>

If authentication is set improperly, the system displays an error message and switches to the default settings, with authentication by Exigen Workflow and connection to database using the `visi.ini` file.

If the user tries to authenticate using an authentication mode that is not allowed, the system displays an error message and terminates the work session.

Switching between Database Users

To switch between database users, select **Administrator > System > User Setup**. The system asks whether to delete the previous database user. If you do not delete the previous database user, that user is disabled.

Multiple Database Servers and Database Authentication

Exigen Workflow allows administrators to create projects on a database server other than that of the master database. This approach is not recommended for the following reasons:

- Synchronization between databases may result in difficulties.
- The workload consumed by database management is greater.

There are also functionality limitations when using authentication by database.

If you are adding a new project on a different database server by the create/import/copy option, note that the system allows you to create a project without database accounts. It also allows you to create database accounts for all users with useless passwords because it is not possible to extract the password from the database server. If the project is created without database accounts, the database administrator must create these accounts.

In both cases, the system administrator must synchronize the password for each database account using database tools on all required database servers, or using Exigen Workflow Administrator. In Exigen Workflow Administrator, you can change the password in the user configuration window, and the system automatically changes the password on all affected database servers.

Performing a Single Login

To perform a single login, proceed as follows:

1. Configure the ODBC source and ensure that the connection is authenticated by SQL Server using a login ID and password.
2. Verify that the Exigen Workflow administrator has created a user for whom the authentication mode CCID Win32 is allowed.

The user must also have a valid domain name.

3. To ensure that connection information is correct, configure the `visi.ini` file.

For example:

```
[databases]
DBS_MASTER=janist
DBS_USER=SYSADM
DBS_PASSWORD=SYSADM
```

4. In the Windows directory, configure the `visiclt.ini` file:

```
[winclient]
..
authentication_mode=CCID Win32
db_connection_mode=Visi.ini
```

5. Run an Exigen Workflow object, for example, Exigen Workflow Explorer.

The object appears without the login window.

Note: You can use short names when specifying the authentication and connection modes in the `visiclt.ini` file.

Performing a Trusted Login

To perform a trusted login, proceed as follows:

1. Configure the ODBC source and make sure that the connection is authenticated by the current Windows user login.

2. Verify that the Exigen Workflow administrator has created a user for whom the authentication mode CCID Win32 is allowed.

The user must also have a valid domain name and database user type: Windows User.

3. To ensure that the database name is correct, configure the `visi.ini` file.

Database connection information is not required as in the following example:

```
[databases]
DBS_MASTER=janist
```

4. In the Windows directory, configure the `visiclt.ini` file:

```
[winclient]
..
authentication_mode=CCID Win32
db_connection_mode=Trusted
```

5. Run an Exigen Workflow object, for example, Exigen Workflow Explorer.

The object appears without the login window.

Appendix H: How ACL Based Security Affects Documents, Folders, and Subfolders

If ACL based security is implemented, it affects documents, folders, and subfolders, and the operations that can be performed on them. The following topics are described in the section:

- [Inheriting Security Settings](#)
- [Restrictions on Operations with Documents, Folders, Subfolders, and Parcels](#)

Inheriting Security Settings

Documents, folders, and subfolders generated as the result of an editing operation inherit security settings from their parents.

The following list describes how security settings are inherited:

- A reference document inherits security settings from the original document.
- If a parcel is split, the security settings of the documents and folders in the parcel are retained.
- When a new version of a document is created, the new version inherits the security settings of the current document.
- When documents are retrieved from the common queue, security filtering based on folder ACL is applied.

Restrictions on Operations with Documents, Folders, Subfolders, and Parcels

ACL based security imposes the following restrictions on operations with documents, subfolders, folders, and parcels:

- A user can delete a parcel only if the user has permission to delete all documents in the parcel.
- Parcels can be merged only if they belong to the same folder.
- A user can delete a document only if the user has delete permission.
- A user can modify a document only if the user has modify permission.
- A user can edit a document image only if the user has edit permission.
- A user can modify additional document fields only if the user has modify permission for the document.
- A user can modify a folder only if the user has modify permission for the folder.
- A user cannot assign a document to a new or existing folder if the parcel contains one or more documents with denied modify permission for the user.

- To assign a document to a subfolder or document type, the user must have modify permission for that document.
- Default subfolders are shared objects, so their security settings are global within the project. Changes in default subfolder access rights affect default subfolders in all folders.
- When viewing a parcel or folder, the user can see only the documents for which the user has view permission.
- A user can send a document by email only if the user has view permission for that document.
- A user can display a document or image only if the user has view permission.
- A user cannot send a parcel to a user who lacks read permission for that folder.
- A user cannot distribute a parcel to another user who lacks read permission for the parcel.
- If a document is to be split and the **Delete original document** option is selected, a user must have delete and edit permissions for the document. If the **Delete original document** option is cleared, a user must have edit permissions for the document.
- If a user lacks access to particular privileges for documents, and the documents to be merged have these inaccessible privileges, the inaccessible privileges in the documents must be the same in order for the user to merge them.
- If the pages in a document are to be rearranged, and the **Delete original document** option is selected, the user must have delete and edit permissions for the document. If the **Delete original document** option is cleared, the user must have edit permission for the document.
- If a document is to be split by portions, and the **Delete original document** option is selected, the user must have delete and edit permission for the document. If the **Delete original document** option is cleared, the user must have edit permission for the document.
- A user can delete a page only if the user has edit permission for the document.
- A user can undelete a page only if the user has edit permission for the document.
- A user can copy a document only if the user has view permission for the document.
- When retrieving a parcel list, only those parcels are displayed for which the user has read permission for the associated folder.
- When retrieving a document list, only those documents are displayed for which the user has read permission for the document, folder, and subfolder.
- When retrieving a folder list, only those folders are displayed for which the user has read permission.
- When retrieving a subfolder list, only those subfolders are displayed for which the user has read permission for the folder and subfolder.
- When retrieving a subfolder list for default subfolders, only those subfolders are displayed for which the user has read permission.
- A user can print a document only if the user has read and view permissions for the document.
- A user can print an entire folder only if the user has read permission for the entire folder and view permission for all folder documents.

Glossary

Glossary	
Term	Explanation
A	
access control entry	<p>Permission and global group associated with a privilege in the ACL based security scheme.</p> <p>When a user assigns a privilege to a workflow resource, access control entries associated with that privilege define which users or groups can perform which actions with the workflow resource.</p> <p>See also: <i>ACL based security, global group, permission, privilege, resource.</i></p>
access control list	<p>List of access control entries associated with a workflow resource that defines the security restrictions for system users in the ACL based security scheme.</p> <p>See also: <i>ACL based security, access control entry, resource.</i></p>
ACE	See <i>access control entry</i> .
Active Directory Synchronization Service	Service that retrieves and synchronizes user data so that users registered outside the Exigen Workflow system are not required to be registered individually by an Exigen Workflow administrator.
ACL	See <i>access control list</i> .
ACL based security	<p>Exigen Workflow security scheme for specifying security restrictions on individual documents, folders, and subfolders. In the ACL based security scheme, users assign privileges to restrict actions that can be performed on workflow resources.</p> <p>See also: <i>privilege.</i></p>
ACL security entry	See <i>access control entry</i> .
active status	State in which a parcel can be processed. Unless otherwise specified, all parcels in the workflow are assigned active status.
activity	Event or sequence of events that occurs automatically as scheduled by the system administrator.
ad hoc node	Node that can exchange parcels with another ad hoc node from the same group without being connected with workflow links. In Workflow Builder, ad hoc nodes are identified by a yellow mark in the lower left corner.
Administrator	Application that performs administrative tasks in Exigen Workflow.
ADSync	See <i>Active Directory Synchronization Service</i> .
Advanced Event Server	<p>Automatic workflow object that performs custom events on parcels sent through the workflow. The events replace manual processes and are transparent to the end user.</p> <p>Advanced Event Server is replaced by Automatic Queue Server, and should not be used for new applications.</p> <p>See also: <i>Automatic Queue Server.</i></p>
annotation	<p>Element assigned to a document image by document reviewers in Image Viewer.</p> <p>See also: <i>Image Viewer.</i></p>

Glossary	
Term	Explanation
Application Services	Service that provides access to the Exigen Workflow data store. Application Services is required by Advanced Event Server and Automatic Queue Server. See also: <i>Advanced Event Server, Automatic Queue Server.</i>
audit	Exigen Workflow mechanism that records activities and errors in the Exigen Workflow system. See also: <i>Audit Server, Audit Viewer.</i>
audit filter	Set of conditions that define the audit data collected by the Exigen Workflow system.
Audit Server	Automatic workflow object that synchronizes DMS file audit data with the Exigen Workflow database. See also: <i>audit, DMS.</i>
Audit Viewer	Application for viewing Exigen Workflow audit records. See also: <i>audit.</i>
authentication	Method to identify Exigen Workflow users and grant access to system applications and resources. See also: <i>CCID Win32 authentication, database authentication, Genesys authentication, Win32 authentication, workflow authentication.</i>
Automatic Queue Server	Automatic workflow object that processes parcels in background mode without user interaction. Automatic Queue Server can be mapped to multiple custom scripts that implement customer-specific business logic. Automatic Queue Server handlers can be set up to process events. See also: <i>event, Exigen Workflow handlers.</i>
B	
bar code	Graphical machine-readable lines of varying widths. In Exigen Workflow documents, bar codes encode indexing information. See also: <i>Barcode Server.</i>
Barcode Server	Automatic workflow object that reads document bar codes and populates document index fields with the extracted information. See also: <i>bar code.</i>
batch	Group of documents that are scanned into the system together. This is the initial life cycle stage for scanned documents. See also: <i>scanning.</i>
C	
Capture Desktop	<i>See Interactive Document Capture Desktop.</i>
Capture Server	<i>See Interactive Document Capture Server.</i>
CCID Win32 authentication	Authentication mode that allows users to be authenticated by the current Windows user identity. Users are not required enter a login and password to access the Exigen Workflow system. This mode is also known as single sign-on.
Check Document Utility	Application to check the integrity of images in the system. If corrupt images are located, they can be sent to a specific node and user for special handling.
check-in and check-out	Functionality that prohibits documents from being modified by more than one user at a time.

Glossary	
Term	Explanation
Clear Cache Utility	Application to clear specific cache directories used to retrieve, edit, and view committed documents. See also: <i>committing</i> .
cluster index	Index that combines similar data in specific areas of the database. See also: <i>unique index</i> .
COM	Identifier of the default common user. See also: <i>common user</i> .
committing	Action to archive processed documents to a predefined storage medium. Committing is performed by the Commit object. See also: <i>Commit</i> .
Commit	Workflow object that archives documents to a predefined storage medium, such as an optical disk, magnetic file storage, or a third-party file storage system.
common user	Virtual user used as a common repository for documents that are sent to a specific group of users doing similar work. Users can access documents sent to the common user if they belong to the same workflow group. See also: <i>regular user, workflow group, COM</i> .
Component Configuration Manager	Application that creates and manages reusable workflow components such as plugins, applications, and nodes, which can be inherited by other components.
Configuration Browser	Application that manages configurations of Exigen Workflow components.
configuration schema	Template for a configuration section in Configuration Browser. Only the configuration parameters and items defined in the schema can be included in the configuration section.
corporate location	Definition of a geographical location or branch office where users are located. If a company has many employees performing the same functions in different cities, corporate locations can be used to restrict the destinations where parcels are sent.
D	
database authentication	Authentication mode that requires users to enter a login and password of the database account to access the Exigen Workflow system.
diagnosis	In E-Capture, a set of error codes that address typical business processing problems. For example, a diagnosis is used to automatically route documents that are missing required information.
Distribution Server	Workflow object that exports image files and database records from one database to another.
DMS	Internal Exigen Workflow file format to store document images and annotations. See also: <i>document image, annotation</i> .
DMS Viewer	See <i>Image Viewer</i> .
document	Most basic object in Exigen Workflow, either an image of a scanned document or an electronic document created using applications such as Notepad or Word. Documents can also be imported using Import Server, produced by Enterprise Report Management systems, or delivered by email. See also: <i>Enterprise Report Management, Import Server, scanning, task</i> .

Glossary	
Term	Explanation
document context security level	Security element associated with a global group that defines which users can perform which actions with document image editing tools in Image Viewer. See also: <i>global group, Image Viewer.</i>
document image	Image of a scanned or virtually printed document.
document type	Category assigned to Exigen Workflow documents for indexing purposes and for protecting documents against unauthorized users. See also: <i>indexing, document.</i>
document versioning	Feature that allows Exigen Workflow users to maintain different document versions.
E	
E-Capture	Set of applications used to extract index information and import PDF and PCL documents into Exigen Workflow. See also: <i>E-Capture Administrator, E-Capture Definition Utility, E-Capture Server, E-Capture Split Server.</i>
E-Capture Administrator	Application that configures and manages the E-Capture environment. See also: <i>E-Capture.</i>
E-Capture Definition Utility	Application that prepares E-Capture form templates for data recognition and extraction. See also: <i>E-Capture.</i>
E-Capture Server	Automatic workflow object that captures indexing information from PDF and PCL files. See also: <i>E-Capture.</i>
E-Capture Split Server	Optional E-Capture module that extracts small portions from PCL files and sends them to E-Capture Server for further processing. See also: <i>E-Capture.</i>
Empty Folders Maintenance Utility	Application that creates a file listing all folders to which no documents are assigned. This helps administrators identify and delete empty folders to free up space in the database. See also: <i>folder.</i>
Enhanced Form OCR	Exigen Workflow based module for processing electronic forms that includes optical and intelligent character recognition and data extraction. See also: <i>Form Template Builder.</i>
Enterprise Report Management	Set of applications used to capture, index, and store report print streams in Exigen Workflow. See also: <i>ERM Indexer, ERM Setup, ERM Storage Maintenance, Report Definition Wizard.</i>
entitlement	Element in the ACL based security scheme associated with a privilege. An entitlement defines a set of rules by which privileges can be assigned to workflow resources automatically. See also: <i>ACL based security, privilege.</i>
ERM	See <i>Enterprise Report Management.</i>

Glossary	
Term	Explanation
ERM Indexer	Workflow object that imports data from report files into the Exigen Workflow system according to the parameters defined in the ERM Setup object. See also: <i>Enterprise Report Management, ERM Setup.</i>
ERM Report Viewer	Application used to view and annotate ERM reports in text format. See also: <i>Enterprise Report Management.</i>
ERM Report Queue Monitor	Component used by ERM Indexer to acquire an AS/400 report printstream directly from an AS/400 output queue. See also: <i>Enterprise Report Management, ERM Indexer.</i>
ERM Setup	Workflow object that registers report files, models, and templates for processing in Enterprise Report Management using ERM Indexer. See also: <i>Enterprise Report Management.</i>
ERM Storage Maintenance	Workflow object used to move ERM storage files from the original location to any other location on the network, including optical storage. See also: <i>Enterprise Report Management.</i>
Escalation Server	Automatic workflow object that routes parcels through the workflow depending on time restrictions on how long parcels remain in a specific node.
event	Predefined, automatic action performed on parcels. Events are assigned to links between workflow nodes. An event is activated when a parcel travels through the associated workflow link. See also: <i>Event Server, link, node, Automatic Queue Server.</i>
Event Server	Automatic workflow object that processes events when parcels travel through workflow links. Event Server is replaced by Automatic Queue Server, and should not be used for new applications. See also: <i>event, link, Automatic Queue Server.</i>
Exigen E-Forms	Application that captures information in electronic forms via the Internet.
Exigen Integrator	Application to connect to and retrieve data from disparate sources.
Exigen E-Mail	Web application used by company employees to perform the following tasks: <ul style="list-style-type: none"> • receive and send emails, including sending email responses automatically • maintain incoming and outgoing email history • maintain the rules and events system to process the emails • maintain the knowledge base used for composing and responding to emails
Exigen Workflow	Customizable workflow management and document imaging system. Exigen Workflow enables system administrators to create workflow applications for solving document management problems. End users use these applications to scan, import, index, view, route, archive, and retrieve documents.
Exigen Workflow Explorer	Application to launch Exigen Workflow objects and configure the user desktop.
Exigen Workflow handlers	Handlers that use Automatic Queue Server processes to perform workflow jobs. Exigen Workflow handlers can be used in place of Exigen Workflow servers.
Exigen Workflow Web	Exigen Workflow web solution that allows users to perform basic operations in the Exigen Workflow system through a web browser. See also: <i>Exigen Workflow.</i>

Glossary	
Term	Explanation
expired status	Status given to a parcel after the due date and time are reached. See also: <i>parcel</i> .
F	
FIX	Identifier of the default fix user. See also: <i>fix user, Fix Queue</i> .
Fix Queue	Queue that handles batches or parcels that cannot be correctly processed in the workflow. See also: <i>fix user, FIX</i> .
fix user	Virtual user to whom other users send defective documents. See also: <i>FIX, Fix Queue</i> .
folder	Level in the document indexing hierarchy. In Exigen Workflow, folders can contain documents and subfolders. Users can retrieve documents based on assigned folder field values. See also: <i>indexing, subfolder</i> .
folder and subfolder security group	User group that restricts access to individual folders and subfolders in the role based security scheme. See also: <i>folder, role based security, subfolder</i> .
form	Document with a specific graphical pattern that can be used for automatic extraction of indexing information. See also: <i>Enhanced Form OCR, form OCR, optical character recognition</i> .
form category	In E-Capture, a logical grouping of forms within a policy type. For example, all form types used for customer evaluation can be grouped as a form category named Evaluations.
Form Index Server	Automatic workflow object that populates the database with data extracted from forms during the form OCR process. See also: <i>form, form OCR</i> .
Form Template Builder	Component that creates form templates used to extract information from incoming scanned documents using OCR. The incoming documents are forms such as loan applications or insurance claims. The templates define the data to be extracted from the forms by Enhanced Form OCR. See also: <i>Enhanced Form OCR</i> .
form OCR	Process in which the Exigen Workflow system performs optical character recognition in forms, extracts text information, and populates the database with data from defined form zones. See also: <i>form, optical character recognition</i> .
Form OCR QA	Workflow object that verifies and corrects data extracted from forms during the form OCR process. See also: <i>form, form OCR</i> .
Form OCR Server	Automatic workflow object that extracts OCR data from incoming documents based on predefined form templates. See also: <i>form, form OCR</i> .

Glossary	
Term	Explanation
form overlay	Presentation form to display ERM reports. See also: <i>Enterprise Report Management.</i>
FTS	See <i>full text search.</i>
FTS Maintenance Utility	Application that configures FTS settings in projects. It defines stopwords and the algorithm for splitting extracted text into words, and detects documents that are not correctly processed. See also: <i>FTS Preprocessor, full text search, stopword.</i>
FTS Preprocessor	Automatic workflow object that extracts text from each page of every document sent through the workflow. It performs OCR on images, and uses other methods for other file formats, including DOC, PPT, XLS, and PDF. Custom Conversion Engine plugins can be developed for specific formats. Document search and retrieval can be performed based on the document text. See also: <i>FTS Server, full text search, optical character recognition.</i>
FTS Server	Automatic workflow object that works with FTS Preprocessor and creates an index used for full text searches.
full text search	Functionality used to retrieve documents based on words or phrases in the document text. See also: <i>FTS Preprocessor, FTS Server.</i>
G	
Genesys authentication	Authentication mode that allows Genesys users who are logged on to a Genesys desktop application to access the Exigen Workflow system without additional Exigen Workflow authentication.
global group	In the role based security scheme, groups that are used together with document context security levels to restrict the actions that specific users can perform with image editing tools in Image Viewer. In the ACL based security scheme, global groups are used together with permissions and privileges to restrict actions that specific users can perform with individual workflow resources. Global groups are also used to synchronize users with groups of external user systems. See also: <i>ACL based security, document context security level, Image Viewer, permission, privilege, role based security, synchronization.</i>
H	
handlers	See <i>Exigen Workflow handlers.</i>
High Volume Index	Workflow object to manually index workflow documents. See also: <i>indexing.</i>
High Volume Scan	Workflow object that scans paper documents into the Exigen Workflow system as electronic images. See also: <i>document image, scanning.</i>
hold status	Status for parcels that must wait until the hold time is over. These parcels become active after the hold time expires. See also: <i>hold time, parcel.</i>

Glossary	
Term	Explanation
hold time	Period during which parcels assigned to be processed are held prior to processing. See also: <i>hold status, parcel.</i>
I	
Image Enhancement Server	Automatic workflow object that improves document image quality. See also: <i>document image.</i>
Image Viewer	Application for viewing and annotating document images. See also: <i>annotation, document image.</i>
Import Server	Automatic workflow object that imports external documents and faxed images into the Exigen Workflow system without scanning. Import Server can also import index information and convert different file formats into DMS by printing the document through a virtual printer. See also: <i>DMS, scanning.</i>
imprint	Electronic marking that can be automatically added to each page of a scanned document image. An imprint can include information such as the Exigen Workflow project name and the current user's name.
indexing	Process of assigning documents to folders, subfolders, and document types so that the documents can be identified, classified, and retrieved by users based on assigned index values. See also: <i>document, document type, folder, subfolder.</i>
Inspect	Workflow object that verifies if document images and indexing information meet quality standards.
Integrated Security Management Console	Web-based application that administers Exigen Security Services policies for Exigen applications in directory services.
Interactive Document Capture	Application that captures documents from external applications, indexes the documents, converts the documents if required, and submits them to the appropriate location in Exigen Workflow as designated by the user. See also: <i>Interactive Document Capture Desktop, Interactive Document Capture Server.</i>
Interactive Document Capture Desktop	Client application that captures external files, indexes them, and sends them to Interactive Document Capture Server. See also: <i>Interactive Document Capture, Interactive Document Capture Server.</i>
Interactive Document Capture Server	Set of components that are run in the Automatic Queue Server environment to automatically perform tasks such as the following: <ul style="list-style-type: none"> • receive files prepared by Capture Desktop or another application • convert files to another file format • split files • import files into Exigen Workflow projects • send emails See also: <i>Interactive Document Capture, Interactive Document Capture Desktop.</i>
interaction script	Series of prompts that guide a user through a task. Interaction scripts are created using Exigen Interaction Script Builder.
L	

Glossary	
Term	Explanation
link	Connection between two nodes on a workflow map. See also: <i>node, workflow map.</i>
Low Volume Scan	Workflow object that combines the functionality of the High Volume Scan and High Volume Index nodes. Low Volume Scan also is used to retrieve documents from optical storage or an image server. See also: <i>High Volume Index, High Volume Scan, image server, indexing, scanning.</i>
N	
node	Element on a workflow map that represents a step in the document processing life cycle. Each node is associated with a particular business task that can be performed with documents. See also: <i>workflow map.</i>
O	
OCR	See <i>optical character recognition.</i>
optical character recognition	Text recognition in a document image. See also: <i>Enhanced Form OCR, form OCR, full text search.</i>
Orphan Utility	Application used to identify discrepancies between information in the database and in file storage.
output group	In Exigen E-Capture, a group of fields that contain text to be captured.
overlay	Predefined image added to a document image for presentation purposes. For example, the overlay image can include the company logo or headings.
P	
page	Image of a physical document page.
parallel parcel	Parcel sent to more than one node and user. See also: <i>node, parcel.</i>
parcel	Package of one or more documents transferred through the workflow.
pending parcel	Current parcel that is placed on hold, awaiting a required document.
permission	Element in the ACL based security scheme that defines a generic level of access to a workflow resource type. Permissions are combined with global user groups and privileges to define ACL security entries. See also: <i>ACL based security, ACL security entry, global group, privilege.</i>
policy type	In E-Capture, a group of form categories. For example, a policy type named Payments contains the following form categories: <ul style="list-style-type: none"> • Invoices • Receipts • Account Statements
Print Monitor	Application for managing print jobs in all registered print devices in Print Server. See also: <i>Print Server.</i>
Print Server	Application that schedules print jobs on registered printers to improve printing efficiency in Exigen Workflow. See also: <i>Print Monitor.</i>

Glossary	
Term	Explanation
privilege	<p>Element in the ACL based security scheme. Users assign privileges to individual workflow resources to define which actions can be performed by which users.</p> <p>See also: <i>ACL based security, entitlement, permission, global group, resource.</i></p>
processflow	<p>In Task Oriented Workflow, a type of taskflow that describes a high level business process and controls its execution.</p> <p>See also: <i>Task Oriented Workflow.</i></p>
Process Monitor	<p>Application for viewing and managing user connections to workflow objects in the Exigen Workflow system. System administrators can see who is logged onto which workflow object. Process Monitor is also used to unlock workstations that are improperly or incompletely logged out of a specific node.</p>
project	<p>Business process data scheme that contains a collection of database tables and settings that define how documents are processed in all workflows that belong to the project.</p> <p>See also: <i>workflow, Project Builder.</i></p>
project table	<p>Default or custom table associated with an Exigen Workflow project.</p>
Project Builder	<p>Application for creating and configuring projects.</p> <p>See also: <i>project.</i></p>
Publisher	<p>Set of applications used to create, export, and view document collections outside the Exigen Workflow system.</p> <p>See also: <i>Publisher Cabinet, Publisher Collector, Publisher Packager.</i></p>
Publisher Cabinet	<p>Application to view document collections that are exported from the Exigen Workflow system. Publisher Cabinet is run separately from Exigen Workflow and does not require a connection to the database.</p> <p>See also: <i>Publisher.</i></p>
Publisher Collector	<p>Application to collect documents from Exigen Workflow into a document package that can be distributed outside the Exigen Workflow system.</p> <p>See also: <i>Publisher.</i></p>
Publisher Packager Utility	<p>Application to distribute document collections outside the Exigen Workflow system.</p> <p>See also: <i>Publisher.</i></p>
Push Server	<p>Automatic workflow object that sends documents to the next node and user according to defined routing rules.</p> <p>See also: <i>node, routing rules.</i></p>
Q	
queue	<p>See <i>node</i>.</p>
Queue	<p>Workflow object that uses external applications for document processing. Queues are also used for implementing custom business logic in a workflow.</p>
Queue Server Console	<p>Application that performs tasks such as creating, starting, and stopping Automatic Queue Server jobs.</p> <p>See also: <i>Automatic Queue Server.</i></p>
R	

Glossary	
Term	Explanation
recycling bin	Logical container of Exigen Workflow documents that are marked for deletion. Documents are physically removed from the database and document storage systems only when Retention Server deletes them from the recycling bin. See also: <i>Retention Server</i> .
reference document	Document that exists only as a reference to another document.
regular user	Person who uses the Exigen Workflow system for daily business tasks. A user is authenticated by a user name and password. See also: <i>authentication</i> .
Remote Storage Server	Application that accesses and manages Exigen Workflow documents at a remote location.
rendezvous parcel	Parcel waiting to be reunited with its respective parallel parcels in a specific rendezvous node. See also: <i>node, parcel</i> .
report	Document processed by Enterprise Report Management objects. See also: <i>Enterprise Report Management</i> .
Report Definition Wizard	Application that creates templates to extract data from reports in ERM objects. See also: <i>Enterprise Report Management</i> .
Report Queue Monitor	See <i>ERM Report Queue Monitor</i> .
report template	Data presentation layer used by the ERM Indexer and ERM Storage Maintenance objects to index ERM reports, and by the Queue object to retrieve and view ERM reports. See also: <i>Enterprise Report Management, Queue</i> .
resource	In ACL based security, a workflow resource such as a document, folder, or subfolder.
Retention Server	Automatic workflow object that manages the disposal of outdated documents and other documents that are marked for deletion. See also: <i>recycling bin</i> .
Retrieve	Workflow object that performs a search for project documents, subfolders, and folders based on index values or a full text search. See also: <i>document, folder, indexing, subfolder</i> .
role based security	Exigen Workflow security scheme in which access to workflow objects is restricted by security levels, and access to individual folders and subfolders is restricted by folder and subfolder security groups. See also: <i>folder and subfolder security group, security level</i> .
routing rules	Rules that define which documents can be sent to which nodes based on document index values. Routing rules are associated with workflow links. See also: <i>link</i> .
RSS	See <i>Remote Storage Server</i> .
S	
scanning	Process of capturing physical documents as document images to import into the Exigen Workflow system. See also: <i>High Volume Scan, Low Volume Scan</i> .

Glossary	
Term	Explanation
security entry	See <i>access control entry</i> .
security level	Security element that defines what actions users can perform in each workflow object. Each user is assigned a security level.
single login	See <i>CCID Win32 authentication</i> .
single sign-on	See <i>CCID Win32 authentication</i> .
skill	Rules that allow managers to evaluate if specific user abilities are required to process parcels. Skill rule definitions are based on parcels, and they are different for each project.
stamp	Rubber stamp image that users can add to document images. See also: <i>Stamp Management Utility</i> .
Stamp Management Utility	Application that manages stamp images. See also: <i>stamp</i> .
Statistics	Application that monitors statistical information on user actions and processed documents.
stopword	Word that is ignored when building a full text search index. See also: <i>full text search</i> .
subfolder	Level in the document indexing hierarchy. In Exigen Workflow, subfolders contain documents and are usually assigned to folders. Users can retrieve documents based on assigned subfolder field values. See also: <i>document, folder, indexing</i> .
synchronization	Process of synchronizing Exigen Workflow users with external user systems, such as Windows domains. The status of synchronized users is automatically updated according to the situation in the external environment. Synchronizing can also be used to automatically update a user association with global groups.
T	
task	In an Exigen Workflow object, an external application, such as Word, that is used to process Exigen Workflow documents. In Task Oriented Workflow, a task is a custom business function associated with a parcel. A task must be completed as part of the document processing procedure. See also: <i>Task Oriented Workflow</i> .
task list	In Task Oriented Workflow, a list of business functions that must be completed before the associated parcel can travel further in the workflow. See also: <i>task, Task Oriented Workflow</i> .
task object	See <i>task</i> .
Task Oriented Workflow	Exigen Workflow based solution that automates business activities using an electronic task list on the user's desktop. See also: <i>task, task list, taskflow, Taskflow Server</i> .
Taskflow Server	Workflow object that processes tasks and automatically sends parcels to the next workflow node when all required tasks are completed in taskflow nodes. See also: <i>Task Oriented Workflow</i> .

Glossary	
Term	Explanation
Task Oriented Workflow Engine	Handler that performs automatic operations on parcels in queues and marks the parcels as processed. Task Oriented Workflow Engine contains a script that replaces Taskflow Server with an Automatic Queue Server job. See also: <i>Exigen Workflow handlers.</i>
taskflow	In Task Oriented Workflow, a sequence of tasks in a business transaction represented as a workflow map. See also: <i>Task Oriented Workflow.</i>
Template Management Utility	Application to create and maintain form templates for form overlays, optical character recognition, Enhanced Form OCR, and document attachments. See also: <i>Enhanced Form OCR, form OCR, optical character recognition, overlay.</i>
tile	Smaller image of the document page used for navigation purposes in Image Viewer. See also: <i>Image Viewer.</i>
Transfer Utility	Application to transfer the document image file location from one storage location to another.
U	
unique index	Combination of fields that define an index for a specific Exigen Workflow table. See also: <i>cluster index.</i>
Usage Logging Server	Service that provides information on the number of instances of Exigen Workflow applications running on a given day.
user	Exigen Workflow user. See also: <i>common user, regular user.</i>
Users Synchronization Setup	Application that configures Active Directory Synchronization Service and sets up log levels, security levels, timeouts, default passwords, and notifications. See also: <i>Active Directory Synchronization Service.</i>
V	
versioning	<i>See document versioning.</i>
W	
Win32 authentication	Authentication mode that requires users to enter the login and password of an existing Windows account to access the Exigen Workflow system. This authentication mode is available only in Exigen Workflow Web.
work item	Parcel being processed in a workflow.
Work Item Submitter	Workflow object that performs all Retrieve object functions and can create a parcel of referenced documents that is forwarded in the workflow. See also: <i>Retrieve.</i>
workflow	Design of a document flow in a business organization. A workflow consists of nodes and links. See also: <i>link, node, workflow map.</i>
workflow authentication	Authentication mode that requires users to enter the login and password of an existing Exigen Workflow account to access the Exigen Workflow system.
Workflow Builder	Application that builds and manages workflows and configures node settings. See also: <i>workflow.</i>

Glossary	
Term	Explanation
workflow group	Set of users used to limit access to workflow nodes. Workflow nodes are associated with specific workflow groups to define which users can access which workflow nodes.
workflow link	See <i>link</i> .
workflow map	Graphical representation of a workflow. See also: <i>workflow</i> .
Workflow Monitor	Application to monitor and manage processes in workflows.
workflow object	Exigen Workflow application associated with a specific workflow node. See also: <i>node</i> .
Workflow Simulator	Mode used to test a workflow and log in to multiple queues as multiple users.
workflow submap	Workflow within the main workflow represented by a single icon. Submaps are used in cases when workflows are particularly complex. See also: <i>workflow</i> .
Workflow Viewer	Application used to view workflow maps in read-only mode. See also: <i>workflow map</i> .

Index

A

- access control entry
 - definition, 60
- access control lists, 58
 - definition, 59, 60
- ACE, 60
- ACL, 60
- ACL based security, 58
 - activating, 74
 - defining entitlements, 203
 - defining permissions, 206
 - defining privileges, 200
 - defining security entries, 208
 - document access control, 199
 - implementing, 60
 - inheriting security settings, 518
 - restrictions on operations, 518
 - specifying settings, 199
- Active Directory Synchronization Service. *See* ADSync
- activities
 - scheduling, 193
- Activities Scheduler, 193
- Ad hoc groups, 265
- addresses, 135
- administration
 - process overview, 16
- Administration Tools folder, 25
- Administrator
 - simultaneous use, 93
- Administrator tool, 18, 92
- Administrator utilities
 - access, 107
- administrators
 - tasks, 13, 17
- ADSI, 424
- ADSI extensions, 425
- ADSI user group object extensions, 425
- ADSI user object extensions, 425
- ADSync, 19, 420
 - access rights, 434
 - audit events, 440
 - configuring, 424, 427
 - consistency check loop, 439
 - definition, 420
 - installing, 423
 - log level, 429
 - logging function, 422
 - mapper objects, 425
 - mapping, 431
 - mapping examples, 434
 - mapping scripts, 435
 - modifying security levels, 442
 - registering and running, 439
 - security level examples, 442
 - security levels, 441
 - specifying script options, 432
 - synchronization loop, 439
 - synchronizing with directory services, 424
 - user groups, 441
 - user synchronization process, 421
- Advanced Event Server, 149, 282
- aliases
 - creating, 290
 - definition, 290
- annotation security
 - example, 179
 - setting up and using, 178
- annotations
 - access, 108
 - creating secure annotations, 178
- applications, 310
- Applications folder, 25
- Assign Documents to Subfolder
 - event, 282
- Attach page to documents of the defined type
 - event, 282
- audit archive filters, 458
- audit data
 - clearing, 68
 - definition, 476
- audit events
 - ADSync, 440
 - descriptions, 485
 - filters, 505
 - scheduling cleanup, 198
- audit filters, 450
 - defining, 98
 - refreshing, 97
- Audit log housekeeping
 - event, 282
- Audit Log Viewer, 449
- audit logs
 - application audit data, 477
 - context data, 478
 - customizing views, 453
 - data groups, 476
 - event audit data, 477
 - event data, 478
 - searching, 455
 - setting column filters, 454
 - sorting records, 455
 - viewing, 449

- audit records
 - archiving, 457
 - copying, 457
 - deleting, 457
 - exporting, 456
 - filtering, 450
 - refreshing, 457
 - searching, 455
- Audit Server, 505
 - setting up, 505
- audit settings
 - specifying, 97
- Audit Viewer, 19
- auditable events, 476
- audits
 - algorithm, 480
 - configuring, 480
 - local, 481
 - sample audit configuration, 482
- authentication
 - restriction on Exigen Workflow Web, 140
- authentication mode, 510
 - specifying, 139
- Automatic Queue Server, 59, 282
- Automatic Queue Server handlers, 149
- B**
- Barcode Server, 20, 258
- Batch Processing Mode, 365
- batch status option
 - defining, 55
- batches
 - adding batch status values, 55
 - assigning status, 54
 - numeration, 15
- bookmarks
 - using to separate documents, 394
- C**
- Case tool
 - definition, 292
 - using, 292
- CCID Win32 authentication, 140
- Centra, 191
- CENTURA Report Builder, 212
- Check Document Utility, 19
- Clear Cache Utility, 19
- COM aggregation, 424
- Commit, 258
- commit process, 193
- commit types, 68
- common users, 127, 138
- companies
 - adding, 400
 - definition, 399
 - deleting, 402
 - modifying, 401
 - registering, 399
- Component Configuration Manager, 19, 309
 - access, 107
 - adding components, 315
 - buttons and menu commands, 331
 - defining user interface, 318
 - exporting component configurations, 323
 - exporting configuration settings, 323
 - importing component configurations, 327
 - importing configuration settings, 327
 - removing components, 322
 - starting, 311
 - user interface, 312
 - viewing and modifying components, 330
- component configurations
 - exporting, 323
 - importing, 327
- components
 - adding, 315, 320
 - adding an inherited, 321
 - attributes, 315
 - managing, 309
 - modifying, 330
 - removing, 322
 - subtypes, 313
 - types, 313
 - viewing, 330
- Compound Document Mode, 365
- conditions
 - setting for views, 49
- configuration
 - saving, 357, 363, 368
- Configuration Browser, 19, 213
 - access, 107
 - adding a configuration section, 225
 - adding an item, 227
 - buttons, 249
 - closing a view, 224
 - copying and pasting a configuration section, 230
 - definition, 213
 - deleting a configuration section, 227
 - deleting an item, 230
 - displaying and hiding columns, 240
 - editing a configuration file, 233
 - editing a configuration section, 226
 - editing an item, 228
 - exiting, 240
 - exporting a configuration section, 231
 - exporting a view, 230
 - exporting and importing a configuration node, 234
 - exporting and importing configuration data, 233
 - hiding and displaying section columns, 238
 - hiding and displaying the Set View Filter window, 237

- importing a configuration section, 231
- menu commands, 248
- merging configurations, 234
- opening a view, 223
- refreshing a view, 225
- renaming an item, 229
- searching for items or values, 238
- searching for items or values in multiple sections, 239
- setting user preferences, 235
- sorting items in the configuration view, 240
- specifying a configuration view, 220
- specifying an application for merging configurations, 237
- specifying section sorting order, 237
- specifying settings for editing values, 235
- starting, 217
- switching between views, 225
- undoing unsaved modifications, 229
- user interface, 214
- configuration refresh period, 97
- configuration schema, 241
 - creating, 242
 - custom, 241
 - default, 241
 - deleting, 247
 - modifying, 247
 - parameters, 243
 - viewing, 241
- configurations
 - saving, 94, 333
 - viewing and modifying, 213
- corporate locations
 - adding, 130
 - deleting, 131
 - modifying, 131
 - setting up, 127
 - time zones, 128
- Create Parcel Link event, 282
- custom scripts, 402
 - example, 404
 - running, 403
 - setting up, 403

D

- data
 - exporting, 79
 - importing, 83
- data structure, 15
- database authentication, 140, 511, 513
 - configurations, 515
 - multiple database server environment, 515
 - required privileges, 514
- database connection modes

- configuration, 515
- database servers
 - brands, 34
- database tools, 18
 - Project Builder, 18
 - SQL Talk, 18
- databases
 - connecting using OLE DB, 426
 - connection modes, 510, 515
 - DB2, 81
 - implementing authentication, 513
 - names, 30
 - Oracle, 81
 - permissions, 511
 - reconnection settings, 98
 - server names in visi.ini file, 471
 - switching users, 515
 - testing connections, 30
 - updating, 34
 - using non-default, 34
- dates
 - formatting, 469
- default document locations, 63
- default document types, 148
- default password, 430
- designer mode, 304
- diagnoses
 - adding, 397
 - assigning, 396
 - definition, 396
 - deleting, 399
 - modifying, 398
- diagnoses codes, 507
- Diagnoses tool, 396
- dictionaries
 - defining, 318
- Directory/Domain Service (DS), 420
- Distribution Server, 21, 258
- DOCTYPES table, 143
- document access control
 - setting up, 199
- document context security levels
 - adding, 162
 - deleting, 165
 - modifying, 165
 - setting up, 161
 - viewing, 166
- document images
 - specifying locations, 185
- document imaging software, 12
- document management, 69
- document management software, 12
- document notes
 - preventing deletion, 102
- document plugins
 - defining, 319

- document recycling, 16
- document templates
 - associating with document types, 169
 - definition, 148
 - setting up, 148
- document types
 - adding, 167
 - availability, 143
 - defining, 65, 319
 - defining access, 143
 - definition, 143
 - deleting, 168
 - modifying, 168
 - setting up, 166
 - specifying default, 148
- document types feature
 - availability, 166
- document versioning, 523
 - granting user access rights, 62
 - prerequisites, 62
 - setting up, 61
- document versions
 - access rights, 108
- documents
 - definition, 15
 - numeration, 15
 - preventing simultaneous editing, 69
 - separating on the basis of bookmarks, 394
 - setting default location, 63
 - setting up versioning, 61
 - settings for committing, 67
 - specifying settings for committing, 68
 - storing on additional drives, 64
 - types, 15
 - versions, 523
- drives
 - managing, 64
- DS, 420

E

- E-Capture. *See* Exigen E-Capture
- E-Capture Administrator
 - access, 107
- e-forms
 - configuring use, 72
- email
 - setting up, 26
 - specifying format, 70
- email addresses, 135
- emails
 - configuring send functionality, 71
- Empty Folders Maintenance Utility, 19
- end users
 - tasks, 13
- Enterprise Report Management. *See* ERM

- entitlements
 - defining, 203
 - definition, 60
- environments
 - configuring path substitution, 474
- ERM, 17
- ERM Indexer, 21, 258
- ERM Setup, 21, 258
- ERM Storage Maintenance, 21, 258
- errors
 - displaying file processing errors, 416
- ERS, 420
- escalation options
 - specifying, 273
- Escalation Server, 21, 258
- events, 282
 - adding, 150
 - Assign Documents to Subfolder, 282
 - Attach page to documents of the defined type, 282
 - Audit log housekeeping, 282
 - auditable, 476
 - Create Parcel Link, 282
 - defining, 151
 - definition, 149
 - deleting, 152
 - Match, 283
 - Match and push, 283
 - modifying, 152
 - Parallel, 283
 - Parallel and push, 283
 - Pend, 283
 - Print Parcel Documents, 283
 - Push, 283
 - Release Folder Work Item, 284
 - Remove Page Notes, 284
 - Rendezvous, 284
 - Route, 284
 - Send e-mail notification, 284
 - Set cut-off date, 284
 - Set Defaults to Folder Fields, 285
 - Set Defaults to Parcel Fields, 285
 - setting up, 149
 - Split parcel and push, 285
 - Submit Folder Work Item, 285
- Exigen E-Capture
 - companies, 399
 - components, 364
 - custom scripts, 402
 - customization, 365
 - data export, 365
 - defining field types, 368
 - definition, 364
 - diagnoses, 396
 - diagnoses codes, 507
 - error codes, 396

- output details, 375
 - output groups, 372
 - policy types, 383
 - ScriptCalls, 508
 - scripted modules, 405
 - scripts, 411
 - special features, 365
 - supported files, 364
 - vendors, 381
 - Exigen E-Capture Administrator, 18
 - definition, 366
 - starting, 366
 - tasks, 366
 - tool buttons, 368
 - Exigen E-Capture Definition Utility, 20
 - Exigen E-Capture Server, 21
 - Exigen E-Forms
 - integration, 298
 - Exigen E-Mail
 - integration with Exigen Workflow, 91
 - Exigen Workflow
 - administrative process, 16
 - definition, 12, 14
 - exiting, 24
 - purpose, 27
 - servers, 20
 - starting, 22
 - system overview, 14
 - utilities, 17
 - Exigen Workflow
 - buttons, 461
 - customizing, 440
 - customizing functions, 88
 - default tables, 467
 - login in, 22
 - menus, 461
 - setting up, 90
 - Exigen Workflow authentication, 139
 - Exigen Workflow events, 282
 - Exigen Workflow events, 193
 - custom, 194
 - predefined, 194
 - Exigen Workflow Explorer, 18, 24
 - Exigen Workflow Explorer
 - menus and buttons, 461
 - Exigen Workflow security. *See* Security
 - Exigen Workflow Web
 - authentication restriction, 140
 - exporting
 - workflows, 306
- F**
- field types
 - adding, 370
 - CHAR, 36
 - DATE, 36
 - DATETIME, 36
 - defining, 368
 - deleting, 372
 - examples, 369
 - FLOAT, 36
 - modifying, 371
 - SMALLINT, 36
 - TIME, 36
 - uses, 369
 - VARCHAR, 36
 - field values, 13
 - fields
 - adding and modifying, 37
 - customized, 13
 - defining with create/modify by reference, 40
 - deleting, 40
 - length, 36
 - modifying, 39
 - rearranging, 40
 - requirement for entering values, 36
 - fields types
 - INTEGER, 36
 - FileNet, 191
 - files
 - deleting, 26
 - FileTech, 191
 - filters
 - activating, 99, 451
 - applying, 100
 - copying, 101, 452
 - creating, 100, 451
 - deactivating, 451
 - defining, 102
 - defining for global user groups, 158
 - definition, 60
 - deleting, 102, 453
 - editing definition, 453
 - resetting, 451
 - specifying advanced properties, 101
 - types, 451
 - folder history browsing
 - setting up, 250
 - folder snapshots, 250
 - folders
 - definition, 15
 - numeration, 15
 - working with, 15
 - form categories
 - adding, 388
 - defining, 386
 - definition, 386
 - deleting, 390
 - modifying, 389
 - sequencing form categories, 388
 - form executables

- assigning, 269
- Form Index Server, 20, 258
- Form OCR QA, 20, 258
- Form OCR Server, 20, 258
- Form Template Builder
 - definition, 525
- form templates
 - setting up locations, 154
- FTS
 - adding to project, 86
 - definition, 86
 - deleting, 87
- FTS Maintenance Utility, 19
- FTS Preprocessor, 20, 258
- FTS Server, 20, 258
- Full Text Search. *See* FTS
- functions
 - customizing, 88

G

- Genesys authentication, 140
- Genesys Enterprise Routing Solution (ERS), 420
- global user groups
 - adding, 156
 - automatic, 155
 - defining filters, 158
 - definition, 155
 - deleting, 160
 - modifying, 160
 - setting up, 155
 - standard, 155
 - synchronizing, 158
 - types, 155
 - viewing definitions, 160
- graphical mode, 285
- Graphical Queues Workload Monitor, 333
- Graphical Users Workload Monitor, 334
- guide
 - audience, 10
 - purpose, 10

H

- hash passwords, 96
- hidden mode, 304
- hidden nodes, 266
- High Volume Index, 257
- High Volume Scan, 257
- honor event date function
 - enabling, 194

I

- IBM Content Manager, 191
- IEWFExtension interface, 425
- Image Enhancement Server, 21, 258

- image servers
 - activating, 193
 - adding, 190
 - deleting, 193
 - maintaining, 190
 - modifying, 193
 - types, 191
- Import Server, 21, 259
- importing
 - workflows, 308
- index fields
 - requirements, 39
- index values
 - searching, 37
- indexes
 - cluster, 87
 - creating cluster, 88
 - creating unique, 87
 - folder number requirement, 88
 - limitations, 88
 - unique, 37, 87
- indexing, 13
 - setting indexing levels, 64
- information
 - related, 10
- input masks
 - creating, 39
- Inspect, 257
- interaction scripts, 304
- internal counters, 56
- internationalization, 469
 - configuring, 469

J

- job distribution
 - specifying rights, 274
- jobs
 - dealing with problematic, 351
- jukeboxes, 186

L

- link navigation
 - configuration, 250
- links
 - modifying, 288
 - requirements, 122
 - setting up, 278
 - viewing outgoing, 304
- list mode, 286
- locations
 - document, 63
 - setting up, 127, 154
- logging onto another server, 23
- logins
 - maximum number, 96

- multiple, 96
- Low Volume Scan, 257

M

- mandatory tasks, 267
- mapper objects, 425
 - configuring, 431
- masks
 - creating, 38
- MASTER form, 391
- Match
 - event, 283
- Match and push
 - event, 283
- modes
 - Batch Processing, 365
 - Compound Document, 365

N

- navigation
 - between folders, 250
- node plugins
 - defining, 318
- node routing rules
 - defining, 319
- node types
 - Ad hoc, 265
 - None, 265
 - Pending, 265
 - Rendezvous, 265
- nodes
 - adding, 288
 - configuring visibility, 265
 - deleting, 289
 - modifying, 289
 - reusable, 310
 - sorting, 290
- non-default databases, 34
- notification intervals, 26
- null
 - not allowed, 36
- numeration
 - structure, 15

O

- obligatory tasks, 267
- OCR, 20
- OLE DB
 - connecting to a database, 426
- operating costs
 - reducing, 13
- operations
 - restrictions, 61
- optical character recognition, 86

Optical Character Recognition. See OCR

- optical commit type, 68
- optical disk devices
 - adding configuration, 186
 - deleting configuration, 190
 - maintaining, 185
 - modifying directory, 190
- optical storage devices, 185
- Oracle stored procedure, 301
 - creating, 301
- Orphan Utility, 20
- output details
 - adding, 376
 - defining, 375
 - deleting, 380
 - modifying, 378
- output groups
 - adding, 373
 - deleting, 375
 - modifying, 374
 - uses, 372

P

- page notes
 - preventing deletion, 102
- Parallel
 - event, 283
- Parallel and push
 - event, 283
- parcels
 - calculating statistics, 337
 - deleting, 343
 - deleting after commit, 68
 - distributing to another queue and user, 338
 - numeration, 15
 - printing reports, 340
 - reassigning, 339
 - viewing data, 337
 - working with, 16
- passwords
 - changing, 23
 - encrypting, 96
 - expiration, 141
 - generating random, 142
 - setting, 141
 - specifying parameters, 142
 - specifying settings, 95, 140
 - unlocking, 141
- path substitution, 474
 - enabling, 475
 - example, 475
- Pend
 - event, 283
- permissions
 - assigning, 162

- defining, 206
 - definition, 60
 - examples, 206
 - group, 75
 - user, 75
 - phone numbers, 135
 - plugin implementations
 - defining, 319
 - plugins, 309
 - policy types, 383
 - adding, 385
 - defining, 384
 - deleting, 386
 - modifying, 385
 - Print Monitor, 19
 - access, 107
 - Print Parcel Documents
 - event, 283
 - Print Server, 19
 - access, 107
 - privileges
 - defining, 200
 - definition, 60
 - resource type, 202
 - Process Monitor, 18, 358
 - access, 107
 - clearing, 362
 - configuring settings, 360
 - disabling connections, 362
 - ending connection, 361
 - notifying users about ending a connection, 361
 - printing the Process Monitor list, 361
 - sending a message, 361
 - setting the refresh frequency, 361
 - specifying sort order, 362
 - starting, 358
 - updating the connection list, 361
 - processflows, 260
 - productivity
 - improving, 13
 - program tools, 18
 - Exigen Workflow Explorer, 18
 - Project Builder, 18
 - access, 107
 - menus and buttons, 462
 - Project Builder tool, 28
 - PROJECT ID_AUDIT_LOG table, 478
 - PROJECT ID_AUDIT_MSGID table, 483
 - project IDs, 29
 - Project Table Maintenance window
 - menus and buttons, 464
 - project tables
 - maintaining, 34, 182
 - project types, 29
 - audit, 30
 - regular, 29
 - storage, 30
 - projects
 - checking FTS version, 86
 - checking version, 84
 - configuring, 62, 93
 - content, 27
 - copying, 76
 - creating, 27, 28
 - eliminating table discrepancies, 85
 - eliminating version discrepancies, 85
 - exporting, 77
 - importing, 81
 - importing without Project Builder, 81
 - indexing structures, 27
 - names, 30
 - recreating indexes, 57
 - recreating table indexes, 86
 - renaming, 76
 - synchronizing, 84
 - properties
 - defining, 317
 - Publisher Packager Utility, 20
 - Push
 - event, 283
 - Push Server, 21
- ## Q
- QA
 - configuring settings, 66
 - quality assurance. *See* QA
 - Queue, 257
 - queue job statistics
 - viewing, 347
- ## R
- reconnection settings, 98
 - record sequential number, 56
 - recycle bin, 16
 - reference documents
 - specifying settings, 69
 - Registering Modules tool, 405
 - regular form, 390
 - regular users, 138
 - Release Folder Work Item
 - event, 284
 - Remove Page Notes
 - event, 284
 - Rendezvous
 - event, 284
 - Report Definition Wizard, 21
 - reports
 - printing, 210
 - setting up, 210
 - viewing, 354
 - resources

- definition, 59
- Retention Server, 21
- Retrieve, 257
- reusable nodes, 310
- role based security, 57
 - activating, 74
 - implementing, 58
- Route
 - event, 284
- routing
 - rule-based, 13
- routing rules, 272, 293
- RSN, 56

S

- S23_AUDIT_FILTER table, 480, 484
- scanning
 - definition, 13
- schedule of forms, 391
- schedule of locations, 391
- schedule of named insured form, 391
- Scheduled activities adding, 197
- Scheduled activities deleting, 197
- Scheduled activities viewing, 197
- Scheduled activity
 - defining, 197
- script implementations
 - defining, 319
- Script Maintenance tool, 411
- ScriptCalls, 403, 508
 - adding, 409
 - definition, 408
 - deleting, 411
 - modifying, 410
 - registering, 408
 - viewing properties, 419
- scripted modules
 - adding, 406
 - deleting, 408
 - modifying, 407
 - registering, 405
- scripts, 402
 - adding, 413
 - assigning general attributes, 414
 - attributes, 412
 - definition, 403
 - deleting script assignments, 418
 - displaying file processing errors, 416
 - modifying assignments, 417
 - registering, 412
 - selecting file sources, 415
 - viewing properties, 419
- searches
 - Word in Text, 37
- security, 13, 57

- access control, 58
- access to annotations, 108
- access to features, 106
- access to Workflow Monitor, 107
- ACL, 58, 59
- adding levels, 113
- assigning default security, 276
- defining functions in nodes, 276
- document versions, 108
- levels, 58
- modifying levels, 115
- requirement to specify, 112
- restrictions on operations, 61
- role based, 58
- schemes, 57
- specifying access levels, 115
- specifying levels, 103
- specifying password settings, 95
- specifying security level permissions, 111
- specifying security levels, 110
- specifying security scheme, 73
- standard, 57
- task definition, 276
- security entries
 - defining, 208
 - definition, 60
- security levels
 - setting up, 441
 - specifying, 103
- security settings
 - inheriting, 518
- security subjects
 - definition, 59
- Send e-mail notification
 - event, 284
- send options
 - specifying, 272
- separator form, 391
- server commit type, 68
- servers, 19, 20
 - Barcode Server, 20
 - database, 34
 - Distribution Server, 21
 - ERM Indexer, 21
 - ERM Setup, 21
 - ERM Storage Maintenance, 21
 - Escalation Server, 21
 - Exigen E-Capture Server, 21
 - Form Index Server, 20
 - Form OCR QA, 20
 - Form OCR Server, 20
 - FTS Preprocessor, 20
 - FTS Server, 20
 - Image Enhancement Server, 21
 - Import Server, 21
 - logging onto another, 23

- Print Monitor, 19
- Print Server, 19
- Push Server, 21
- Report Definition Wizard, 21
 - specifying connections to multiple, 23
- Set cut-off date
 - event, 284
- Set Defaults to Folder Fields
 - event, 285
- Set Defaults to Parcel Fields
 - event, 285
- setup requirements, 90
- simulator mode, 303
- single login
 - performing, 516
- skill definitions
 - copying, 177
- skill groups, 170
 - defining, 170
- skills
 - assigning to users, 175
 - defining, 171
 - definition, 170
 - implementing, 170
 - setting up, 170
- skills feature
 - availability, 170
- SLAVE form, 391
- software
 - document imaging, 12
 - document management, 12
 - workflow, 12
- space calculation, 30
- Space Calculator, 32
- special forms
 - adding, 392
 - definition, 390
 - deleting, 393
 - modifying, 393
 - registering, 391
- Split parcel and push
 - event, 285
- SQL Talk, 18
- Stamp Management Utility, 20
- Stamp Utility, 152
- stamps
 - definition, 152
 - managing security, 152
 - setting up locations, 154
 - specifying locations, 153
- statistical analysis, 353
 - overview, 353
- statistics
 - queue jobs, 347
 - user jobs, 344
 - viewing, 353, 355

- Statistics application
 - access, 107
- Statistics tool, 18
- storage directories
 - defining, 154
- storage locations
 - maintaining, 185
- stored procedures
 - setting up, 302
- subfolders
 - using default, 65
 - working with, 15
- submaps, 256
 - creating, 292
- Submit Folder Work Item
 - event, 285
- system
 - attributes, 92
- system access features, 107
- system administrators
 - tasks, 13
- system setup, 92, 103

T

- Table Maintenance window, 183
- tables
 - access, 107
 - adding values, 46
 - copying, 47
 - creating, 41
 - customized, 13
 - default, 467
 - deleting values, 47
 - DOCTYPES, 143
 - exporting, 77
 - importing, 81
 - index field requirement, 87
 - internal counters, 56
 - maintaining, 34, 182
 - managing views, 47
 - modifying values, 47
 - reference, 40
 - requirement to create Folder table, 87
 - requirements for index fields, 39
 - S01_USERS, 160
 - setting up, 13
 - specifying permissions, 44
 - specifying settings, 43
 - warning about Folder table, 87
- tablespaces
 - requirements, 81
 - selecting, 84
- task checklists, 304
- task definitions, 124
- task objects

- definition, 144
- setting up, 144
- Task Oriented Workflow, 124, 155, 260, 275, 304
- taskflow directory, 155
- Taskflow Server, 21, 260
- taskflows, 260, 275
- tasklists, 260
- tasks
 - adding, 145
 - assigning actions, 147
 - assigning general properties, 146
 - assigning to nodes, 147
 - in taskflows, 275
 - mandatory, 267
 - setting up, 144, 145
- Template Management Utility, 20
- time zones, 128
 - assigning, 129
 - daylight savings time, 130
 - restriction, 130
 - setting manually, 130
- times
 - formatting, 469
- Transfer Utility, 20
- trigger form, 390
- trusted login
 - performing, 516
- typographic conventions, 11

U

- user groups
 - adding users, 127
 - setting up, 441
 - synchronizing, 126
- user interfaces
 - defining, 318
- user job statistics
 - viewing, 344
- user profiles
 - setting up, 13
- User Synchronization Service. *See* ADSync
- users
 - account status, 141
 - adding, 133
 - assigning document types, 144
 - authentication mechanism, 510
 - common, 138
 - common user COM, 94
 - common user FIX, 94
 - default, 94
 - locking out, 96
 - registering, 309
 - regular, 138
 - regular user DTM, 94
 - remote, 26

- requirement to specify security, 112
- restrictions on reassigning security, 105
- setting up, 132
- specifying authentication modes, 139
- specifying contact information, 135
- specifying general information, 134
- specifying position in company, 136
- synchronization process, 421
- synchronizing, 106, 137
- synchronizing user login data, 420
- tasks, 13
- types, 13
- Users Synchronization Setup, 19
- utilities, 19
 - access, 107
 - Check Document Utility, 19
 - Clear Cache Utility, 19
 - Empty Folders Maintenance Utility, 19
 - Exigen E-Capture Definition Utility, 20
 - FTS Maintenance Utility, 19
 - Orphan Utility, 20
 - Publisher Packager Utility, 20
 - Stamp Management Utility, 20
 - Template Management Utility, 20
 - Transfer Utility, 20

V

- vendors
 - adding a software vendor, 381
 - deleting a software vendor, 383
 - modifying a software vendor, 382
 - registering, 381
- viewer focus
 - setting, 305
- views
 - creating, 49, 50
 - deleting, 49, 52
 - managing, 47
 - modifying, 49, 52
 - setting conditions, 49, 52
 - SQL statements, 51
- visi.ini file, 471
- visiclt.ini file, 469

W

- Win32 authentication, 140
- window types, 48
- Windows script technologies, 424
- WinNT group object extension example, 435
- WinNT user object extension example, 437
- Work Item Submitter, 258
- workflow
 - definition, 255
 - simulating, 303
- Workflow Builder, 18

- access, 107
- definition, 260
- workflow groups
 - adding, 125
 - definition, 124
 - setting up, 124
- workflow links, 256
 - setting up, 278
- workflow map
 - designing, 259
- workflow maps, 256
- Workflow Monitor, 18, 332
 - access, 107
 - configuring node display settings, 343
 - configuring user display settings, 343
 - required permissions, 332
 - restrictions, 332
 - security settings, 332
 - troubleshooting, 332
- workflow nodes
 - granting monitoring rights, 287
 - maintaining, 277
- workflow objects, 256
 - adding, 120
 - Barcode Server, 258
 - classes, 121
 - Commit, 258
 - definition, 119
 - Distribution Server, 258
 - ERM Indexer, 258
 - ERM Setup, 258
 - ERM Storage Maintenance, 258
 - Escalation Server, 258
 - Form Index Server, 258
 - Form OCR QA, 258
 - Form OCR Server, 258
 - FTS Preprocessor, 258
 - FTS Server, 258
 - High Volume Index, 257
 - High Volume Scan, 257
 - Image Enhancement Server, 258
 - Import Server, 259
 - Inspect, 257
 - links, 122
 - Low Volume Scan, 257
 - operations, 109
 - Queue, 257
 - Retrieve, 257
 - running, 289
 - setting links, 122
 - setting up, 119, 263
 - Work Item Submitter, 258
- workflow routing rules
 - setting up, 293
- workflow scripts
 - setting up locations, 154
- Workflow Simulator, 303
- workflow software, 12
- workflow tools, 18
 - Administrator, 18
 - Audit Viewer, 19
 - Exigen E-Capture Administrator, 18
 - Process Monitor, 18
 - Statistics, 18
 - Users Synchronization Setup, 19
 - Workflow Builder, 18
 - Workflow Monitor, 18
 - Workflow Viewer, 18
- Workflow Viewer, 18
 - access, 107
- workflows
 - creating, 261
 - creating in graphical mode, 263
 - exporting, 306
 - importing, 306
 - managing, 332
 - modifying in graphical mode, 285
 - modifying in list mode, 285
 - registering users, 309
 - setting up, 13
 - tips for building, 306
 - types, 260
- workitem plugins
 - defining, 320
- Workload Distribution Monitor, 335, 348
 - dealing with problematic documents, 351
- workstation settings
 - changing, 25
- workstation setup
 - deleting temporary files, 26
 - email, 26
 - notification intervals, 26
 - remote users, 26